Information Security Management in Cloud Computing: a case study

University of Oulu
Faculty of Information Technology and Electrical Engineering
Master's Thesis
Joni Penjala
21. May 2019

Abstract

Organizations are quickly adopting cloud computing in their daily operations. As a result, spending's on cloud security solutions are increasing in conjunction with security threats redirecting to the cloud. Information security is a constant race against evolving security threats and it also needs to advance in order to accommodate the cloud computing adaptation.

The aim of this thesis is to investigate the topics and issues that are related to information security management in cloud computing environments. Related information security management issues include risk management, security technology selection, security investment decision-making, employees' security policy compliance, security policy development, and security training. By interviewing three different types of actors (normal employees, IT security specialists, and security managers) in a large ICT-oriented company, this study attempts to get different viewpoints related with the introduced issues and provide suggestions on how to improve information security management in cloud computing environments.

This study contributes to the community by attempting to give a holistic perspective on information security management in the specific setting of cloud computing. Results of the research illustrate how investment decisions directly affect all other covered topics that in turn have an effect on one another, forming effective information security.

Keywords
Cloud security, ISS training, ISS policy, Security investments, Risk management

Supervisor
Ph.D., Postdoctoral researcher, Xiuyan Shao

Foreword

The interest for this topic grew during my master studies. I am particularly interested in information security, which I find utmost important field of research in ever connecting world. Information security is a constant race against evolving threats and online crime in order to protect information assets, be they organizational or individual.

I would like to thank my thesis supervisor, postdoctoral researcher Xiuyan Shao for the support and mentoring on academic publications. Without her help, the thesis would be quite different and taken longer to complete. I also wish to thank my family and friends for all their support, the participants of the interviews, and my former superior Pekka for helping to find the interviewees.

Joni Penjala

Oulu, May 21, 2019

Abbreviations

ALE	Annual loss exposure
Capex	Capital expenditures
CIA	Confidentiality, Integrity, Availability
CID	Controlled information destruction
CIP	Critical information protection
CISO	Chief information security officer
CSP	Cloud service provider
DoS	Denial of service
ELM	Elaboration likelihood model
ERP	Enterprise resource planning
FMCDM	Fuzzy multi-criteria decision model
IaaS	Infrastructure as a service
IS	Information systems
ISS	Information systems security
OCTAVE	Operationally Critical Threat, and Vulnerability Evaluation
Opex	Operational expenses
PaaS	Platform as a service
PMT	Protection motivation theory
RCT	Rational choice theory
ROI	Return on investment
ROSI	Return on security investment
RTP	Risk treatment plan
SaaS	Software as a service
SRS	Security related stress
UCIT	Universal constructive instructional theory

Contents

1. Introduction

Information security is becoming more and more important every year. This can be seen with increasing investments and priority within organizations worldwide. The spending on information security were estimated to grow from $55 billion in 2011 to $86 billion in 2016 (Cherdantseva & Hilton 2013 Furthermore, in Forrester forecast 2017, the global cloud security solutions spending in 2016 was 1 billion USD, estimated to grow to 3.5 billion USD by 2021 (Adams, 2017). For organizations, a swift to cloud computing means that security threats are also moving and targeted to cloud environments. This becomes the motivation for this study, since both the importance of information security and adaptation of cloud solutions are becoming reality for more and more today's businesses.

Previous research has discussed topics that are related with information security management, but not in a holistic manner. These topics and issues are risk management, security technology selection, investment decisions, policy development and implementation, policy compliance, ISS training, and the phenomenon of chasing the hottest IT.

Risk management is larger process, consisting of multiple subprocesses, contributing to organizations overall IS security. Alberts & Dorofee (2002) have studied and written comprehensive work on managing information security risks. Moreover, Zhang et al., (2010) have proposed a risk management framework based on ISO/IEC 27001 standards that have taken the critical areas of cloud computing into consideration.

Selecting the correct security technology can be hard, possibly resulting in herding behavior amongst individuals when facing decisions (Shao et al., 2019). Multitude of other factors can affect the selection process, such as comparing costs and features of different solutions and reviewing the compatibility with existing systems (Radack (2004). Different decisions models can also be utilized to help stakeholders evaluate potential new investments, like a fuzzy multi-criteria decision model (FMCDM) proposed by Chou et al., (2006). To make investment decisions, two main research streams are covered in literature: decision-theoretic approach and game theory (Shao et al., 2019). Gordon & Loeb (2006) have also previously suggested that organizations can use modified economic models for investments, considering e.g. potential losses from security breaches.

Standards such as ISO/IEC 27001, NIST-SP800, and PCI-DSS can help provide guidelines and best practices to ISS policy development and implementation. It has been shown that organizations may not have trouble translating the best practices from ISS standards to actual ISS policies but fitting them to existing local work culture and way of working (Niemimaa & Niemimaa, 2017). Supporting the argument, Wiander (2007) also states that in order ISS to work properly, it needs to implement in the daily activities of the organization.

The failure to comply with ISS policies is a major concern for organizations. Chen et al., (2012) and Siponen & Vance (2010) explain, that employees are not always motivated to follow the set policies, tend to follow habits, and are resistant to behavioral changes. Moody et al., (2018) reviewed 11 theories, attempting to unify them to explain the issue of compliance. Puhakainen & Siponen (2010) have also previously studied employees' compliance and its improvement through ISS training in organizational setting. The importance of ISS training in improved awareness and compliance has also been recognized by other literature (Hsu, 2009; Karjalainen, 2011).

Lastly Wang (2010) had previously studied IT fashion and the phenomenon of chasing the hottest IT. How it influences organizations performance, reputation and executive compensation, and legitimizes organizations. This is argued to affect the security technology selection process.

Information security is not a single solution but a changing process that reacts to changes in organizational environment. It is pervasive, an interaction between people, process and technology. (Andress, 2003) For organizations, effective information security management requires to include all three aspects. Previous research has only focused on either people, process or technology. To address this research gap, the purpose and contribution of this thesis is the attempt to provide suggestions for organizations and more holistic picture on information security management while focusing on the specific setting of cloud computing.

This study is therefore first one to inspect the problem from all three different perspectives in one study: people, process and technology. To reach this, one main research question and six supporting research questions are formulated:

> RQ 1: What are the factors that should be considered in order to improve information security in cloud computing?
>
> RQ 1.1: How is risk management conducted in an organization?
>
> RQ 1.2: What are the key factors while selecting security technologies?
>
> RQ 1.3: In what investment decisions are based upon?
>
> RQ 1.4: How are ISS policies developed and managed?
>
> RQ 1.5: What affects employees' policy compliance?
>
> RQ 1.6: How is IT fashion related to IS security in cloud computing?

In order to answer these research questions, this thesis is going to interview three different actor categories in a large ICT oriented organization: employees, IT security specialists, and security managers. Each of the actors gives a unique viewpoint to the research problem on how to improve information security within an organization. Employees represent people, IT security specialists represent technology, while security managers are dealing with the process.

The thesis is structured by starting with presentation of prior research on the introduced topics and issues relating to information security management. It gives an overview of the principles of confidentiality, integrity and availability (CIA), cloud computing security and its issues, and about the chosen seven topics relating to information security management. Afterwards, the research methods are discussed with description of the data collection methods (interviews) and the analysis of the data. Findings chapter will illustrate the empirical findings from the interviews, and they are afterwards discussed in relation to the prior research. Theoretical and managerial implications are also presented. It should also be noted, that when the thesis discusses about cloud solutions customers, they can be assumed to be organizations. This thesis does not speak in relation to consumer cloud setting.

2. Theoretical Background

To understand the underlying concepts that are linked to information security management and cloud computing, this chapter introduces different information security models and related concepts. In addition, some of today's cloud computing security issues and challenges are presented. The emphasis will be on the social factors related to organization's cloud security; how employees, IT security specialists and managers are related with it.

2.1 Classification patterns for information security models

Information security is becoming more and more important every year. This can be seen with increasing investments and priority within organizations worldwide. The spending on information security were estimated to grow from $55 billion in 2011 to $86 billion in 2016 (Cherdantseva & Hilton 2013).

> *"Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats"* (Cherdantseva & Hilton, 2013, p. 1).

This definition also incorporates term information system (IS). An information system can be defined as a system which has social and technical aspects. It enables organization to achieve its business objectives with information and communication services. Cherdantseva & Hilton (2013) name six components that makes an IS: information, people, business processes, hardware, software and networks. Last three can also be labeled under ICT tag.

In addition to knowing what is meant by information security and information system in this study, it is important to understand the principles of *confidentiality*, *integrity* and *availability* since these concepts have deep roots in information security. This CIA-triad has been the corner stone in information security since the 1975 where Saltzer and Schroeder differentiated three categories of threats to information (Cherdantseva & Hilton, 2013).

Confidentiality should not be mixed with privacy, although they are similar. It refers to our ability to protect data from those who are not authorized to view it. A simple example of breach in confidentiality is person looking over your shoulder and stealing your password as you type it to a system. Integrity refers to ability to prevent any unauthorized changes to data. To maintain it, one also needs to be able to revert authorized changes to data if required. An example of this is an operating system, requesting permission in order to change some system settings, and offers a way to reverse those settings by authorized person. Availability means that data is accessible whenever needed. Loss in availability can refer to any link in a system that breaks, thus preventing access to data. Basic example is a power loss in IS, or a denial of service attack, which blocks the requests of an authorized party to the data. (Andress, 2014)

One is able to describe and discuss a security issue or a breach with this CIA model alone. Though it is rather basic and restrictive in order to describe any situation in great detail. Thus, upon CIA, more elaborated and comprehensive models have been built. McCumbers cube developed by McCumber in 1991 extends the dimensions of the CIA-triad from one to three.

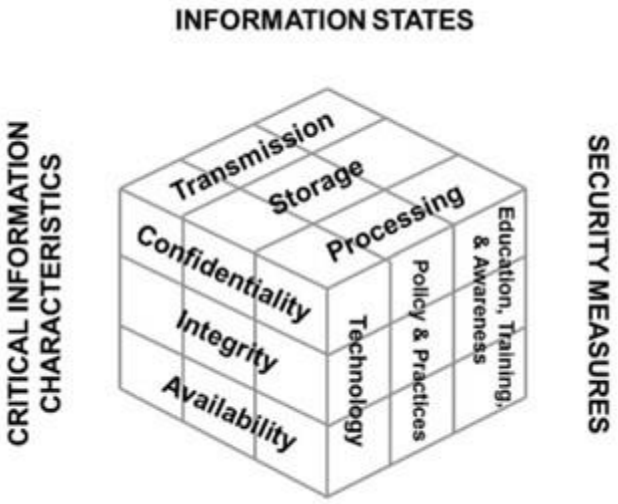

Figure 1. McCumbers Cube

Concerning the dimensions, Cherdantseva & Hilton (2013) explain that there are three distinct building blocks: information states (transmission, storage, processing), critical information characteristics (confidentiality, integrity and availability), and security measures (technology, policy & practices, and education, training and awareness). After this initial model, it has been extended for example by Maconachy et al., (2001) by adding authentication and non-repudiation to the critical information characteristics presented in Figure 1. Curiac & Pachia (2015) argued in their paper about modified model of information assurance for yet another extension in the critical information characteristics: controlled information destruction (CID). But in this thesis, information security can be discussed for good enough extend with the traditional model by McCumber.

Information states

In this context of organization's information security, when defining the phenomenon of data processing, we can reduce what is called 'information' to 'data' (information is ordered or processed data). The information states (transmission, storage, processing) correspond to three groups: data in transit, data at rest, and data in use.

'Data at rest' is data recorded in any storage media, file systems, databases or other storage methods (Securosis, 2010). We can assume this data to be secure, if and only if the data is protected by strong encryption, as in it would take unfeasible amount of time to brute force attack it. The decrypt key must also not be present on the media itself where the data is, or in any node that is associated with that media. The stored key must also be of long enough and incorporate randomness so that it is not vulnerable to dictionary attacks. Hard drive manufacturers are shipping self-encrypting hard drives, which provide automated encryption at minimal cost or performance impact. Encryption hardware is usually preferred over software encryption, due the possibility of attacker stealing the encryption key. (Hasan, 2011; Sen 2015)

‘Data in use’ is all the data that is not at rest or in transit. It is only in one particular node in the network, for example in resident memory or in processor’s memory or cache (Securosis, 2010). To say that this form of data is secure, the access to the memory where it is must only be accessible by the process that read the data from the storage media and wrote it to in example the processor’s memory. There must not be a way to recover this data from anywhere but the original location at rest state in case of killing the process or computer shutdown. This again requires re-authorization. (Hasan, 2011)

‘Data in transit’ is all data being transferred between two nodes in a network (Securosis, 2010). The data can be assumed secure, if both of the nodes, source and receiver are able to protect the data as presented (encryption, access control). Also, the communication between the nodes must be private, where the hosts are identified, authenticated and authorized. There can be no third node in the network that can intercept the communication between the source and receiver. (Hassan, 2011) These are the essentials of the “top” layer of McCumbers cube model as presented in Figure 1.

These information states are areas of concern in traditional information security but are also relevant in cloud security. With cloud security however, there are more areas of security concerns, such as legal and regulatory issues, separation between customers and incident response. These will be discussed in the next section.

2.2 Cloud computing security challenges and issues

Defining cloud computing

The concept of cloud computing has been around for a quite a while now. It has been under endless research around the globe and has been dubbed as next-generation computing revolution. This is due the concerns on success of information systems, communication, virtualization, data availability and integrity, public auditing and information security (Puthal et al., 2015). Cloud computing changes the way information technology is used, and managed, promising improvement in cost effectiveness, faster innovation, shortening the time-to-market, and scalability based on demand (Leighton, 2009). It allows users to rent access to applications, software development environments, and computing infrastructure such as network-accessible data storage and processing (Badger et al., 2011). Mell & Grance (2011) provide the NIST definition for cloud computing model:

> *“…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”* (Mell & Grance, 2011, p. 3)

Organizations are quickly adopting cloud computing in their operations in smaller or larger scale. Today’s cloud service providers also give the option to implement as many features or service models as the organization needs. There are different deployment models, which means that the cloud system can be hosted on the premises of the customer organization *(private cloud)*, shared amongst limited number of trusted partners with *community cloud* (Puthal et al., 2015), or as *public cloud,* where third party hosts publicly accessible service. Depending on the deployment model, the customer organization may have limited amount of private computing resources, or access to large quantity of remote computing resources. This allows the organizations to control the resources: scalability, cost and availability (Badger et al., 2011). *Hybrid cloud* model is a combination of the

former, a mixture of two or more private, public or community clouds (Puthal et al., 2015).

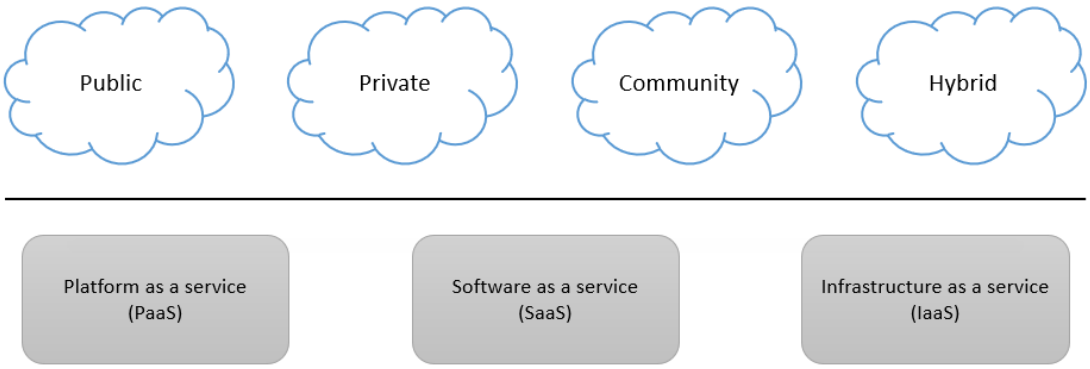

Figure 2. Different cloud solutions (Puthal et al., 2015)

A deployed cloud can provide access to different service models (see Figure 2), such as software as a service (SaaS) or platform as a service (PaaS). Examples of SaaS services are email and office applications. On PaaS, the organization can build their own applications to support their business operations (Badger et al., 2011; Sen, 2015). There is also Infrastructure as a service (IaaS) model, where the organization can gain access to the computing resources and run any operating system and software as they please, in many cases utilizing virtual machines (Puthal et al., 2015).

Few of the features and benefits of cloud computing, as some already introduced are: scalability, virtualizations, reduced IT costs, increased capabilities and reachability of services, and multi-tenancy which allows sharing the same service instance among different tenants. (Puthal et al., 2015; Morsy et al., 2016)

Security challenges and issues

Despite the many potential benefits of cloud computing, organizations face multiple security issues since cloud computing encompasses many different technologies such as networks, databases, virtualization, operating systems, scheduling, transaction management, memory management, and concurrency control (Sen, 2015). It can also be argued, that the cloud is much more vulnerable to risks in terms of confidentiality, integrity and availability than traditional computing (Wang et al., 2012). In Gartner forecast (2018), the cloud market was estimated to be worth 153.5 billion USD in 2017 and estimated to grow by 21.4% in 2018. This of course increases the potential attacker's interest in finding vulnerabilities within the cloud solutions.

Before moving to the more direct cloud security concerns that organizations face, there are few other points of interest and open issues in cloud computing that should be mentioned that are more or less related to cloud security. Morsy et al., (2016) present vendor lock-in and a challenge for organizations. This means that the customer is dependent on products or service vendor and being unable to switch vendors without substantial switching costs. In some cases, it can also mean that the customer is unable to extract data from the cloud if something happens. Sen (2015) also explains that the reason for cloud customer being unable to extract the data may come down to the proprietary format that the cloud provider is using. This can also mean that there is a loss of control for the data since the tools for monitoring who is accessing or viewing the data are not always provided to the customer (Sen, 2015).

Now, relating back to the information states, cloud deployment and service models introduced earlier, cloud computing security issues challenges can be listed from various viewpoints. For example, security issues and challenges related to deployment models, service models, CIA security models or by areas of concern (Sen, 2015; Puthal et al., 2015). Or as Inukollu et al., (2014) categorizes them to: network level, authentication level, data level, and generic types. Looking back at the McCumbers cube model, it is fine to present the issues and challenges in this study in relation to confidentiality, integrity and availability.

Perhaps the most feared security threats organizations may have, are the ones aimed towards the information assets residing within the cloud environments. Confidentiality can be threatened by malicious cloud service provider, or by other customer. Depending on the delivery model, there can be huge number of users accessing the same data: e.g. administrators, software developers, and platform consultants. Trust is therefore an important vector, directly related to the credibility and authenticity of the cloud service provider (Ahmed & Hossain, 2014). External attackers may target the cloud infrastructure and applications, or cloud user organization's endpoint software and hardware via software or hardware attacks. Organization with large data stores, holding for example credit card information, sensitive governmental or intellectual property, are more likely to be targeted by groups with major resources. This can happen by hardware attacks, social engineering (e.g. phishing), and supply chain attacks. Data leakage is a threat caused by human error, or for example faulty hardware. It means an unauthorized transmission of information on external receiver, for example competitor. (Sen, 2015)

Legal issues can also become a security challenge for organizations. With distributed computing resources and data storages, the local geographical jurisdictions can affect the confidentiality if the law enforcement agencies require the organization to disclose encryption keys to enable access to the data (e-discovery). The used encryption technology might also be subject to limitations or requirements, set by the local jurisdiction where the data is physically stored. With geographically distributed resources, sometimes there are also conflicting legal jurisdictions. Migrating data to different location can make configuring the security policies difficult. (Sen, 2015; Ali et al., 2015)

Integrity is threatened with data segregation. Since cloud computing involves multi-tenancy as one of its major characteristics, can incorrectly defined security perimeters, or incorrect configurations of virtual machines pose a threat of data intrusion (Sen, 2015; Rao & Selvamani, 2015). Moreover, poorly implemented or managed user access controls can pose a threat, if for example access rights are not revoked in case of ex-employees (Sen, 2015).

Virtualization is one of the key components of the cloud. It allows same computing resources to be accessed by multiple users simultaneously. There are multiple security issues relating to this, e.g. virtual machines image sharing, isolation, migration, and rollback. The privacy and integrity are a concern due the multi-tenant nature of the cloud. The security strength of the cloud is equal to the weakest entity within it. (Ali et al., 2015)

From availability perspective, change management becomes critical. There is a threat that changes made to the cloud infrastructure by the customer, cloud provider or by any third-party system introduces negative effects, such as loss of access to the data (Sen, 2015). From availability perspective, all types of attacks that are applicable to computer network and the data in transit, is equally applicable to cloud services (Ahmed & Hossain, 2014). One kind of threat is denial of service (DoS) attack. Since all cloud services and

applications use the ordinary underlying Internet to transfer information, data transmission security is of high importance (Puthal et al., 2015).

2.3 Three stakeholders in cloud computing security management and related issues

Although the cloud computing paradigm is somewhat revolutionary shift in information technology, the same information security issues apply to it like in on-premise infrastructure within an organization (Ristov et al., 2012). Also, Zhang et al. (2010) note that many of the risks associated with cloud computing are also found in today's organizations. Of course, new issues rise due the nature of the cloud computing, and organizations are exposed to new risks that are unique to cloud environments. Cloud platforms face internal and external security and privacy threats, such as media failures, bugs, malware, malicious insiders or outsiders. (Ren et al., 2012.) It can be argued, that issues introduced here with the three actors (security managers, IT security specialists, and employees), are relevant and applicable to organizations deploying cloud computing environments as well.

While information systems security has traditionally been viewed as technical issue in ISS research, it can be argued to be too narrow of a view. Information security is not only about technology solutions but social factors, the people who use it. Previously frameworks for security management in organizations have included aspects such as technology and processes. It has been documented by Computer Security Institute (CSI) and FBI that most serious monetary losses in companies have happened due unauthorized insider access. Dhillon & Backhouse also pointed out in their study that information security is a social and organizational issue, because people interact with systems. On certain perspective, as it is also argued in this thesis, it is the humans that have biggest impact on security within organizations and individual systems. Social factors need to be part of the security frameworks proposed and used along with the technological aspects. (Lee et al., 2004; Dhillon & Backhouse, 2000)

Within larger organizations, three distinct groups of actors can be identified, that each have a different role and effect on information security. One way to categorize the actors is through job functions and responsibilities in relation to security: Security managers, IT security specialists, and employees.

2.3.1 Security managers

Security managers are responsible for many aspects of information security management. In this segment, risk evaluation and management, investment decision making, ISS policy development and implementation topics are covered.

Risk evaluation and management

Organizations today have wide selection of complicated computing infrastructures. Flexible methods are required to understand information related security risks and to create appropriate strategies to address those issues. To improve overall security within an organization, security must be considered from multiple perspectives and maintain a continuous effort for improving security posture. (Alberts & Dorofee, 2002.)

Risk evaluation is a process that helps to achieve better security and reach these objectives. When first carried out, risk evaluation gives a baseline of organizations security status, which should be refreshed from time to time (e.g. early or by corporate reorganization). Evaluation activities include identifying security risks that the organization is subjected to, analyzing the identified risks to prioritize them, and plan for protection strategy. This plan includes risk mitigation plans to reduce risks to critical organizational assets as much as feasible. Evaluation in itself only provides results on what steps to take next, organization must follow through and implement the results from the evaluation. (Alberts & Dorofee, 2002.)

A standard quality management (plan-do-check-act) cycle of continuous improvement can be used as a base in order to carry out the activities of planning, implementing, monitoring and controlling, relating to managing information security risks. Information security risk evaluation is the first step in the risk management cycle. It helps organizations to assess organizational practices, installed technology base, and enables the personnel within the organization to conduct information protection practices. Evaluation also has the benefit of presenting selection of cost-effective countermeasures, by balancing the cost, risk against benefits (derived from the negative impact). (Alberts & Dorofee, 2002.)

There are different approaches to conduct risk evaluation within organization. As an example, Alberts & Dorofee (2002) introduced a flexible Operationally Critical Threat, and Vulnerability Evaluation (OCTAVE) approach. It is based on the assumption that ISS is the responsibility of the organization as a whole, not just the IT department and personnel of the organization manage and direct the evaluation themselves. It has three phases: build asset-based threat profiles, identify infrastructure vulnerabilities, and develop security strategy and plans. To proceed with the phases, an analysis team is formed from within the organization's personnel. Zhang et al., (2010) also recommends organizations to use OCTAVE risk analysis to help identify vulnerabilities and threats, in addition to eliminating risk in risk mitigation process (see Figure 3).

For risk management, the framework Zhang et al. (2010) propose, is based on ISO/IEC 27001 standards, developed with critical areas of cloud computing in mind, and attempting to protect confidentiality, integrity and availability of information assets (see Figure 3). It has seven processes, again relating back to the plan-do-check-act cycle: processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review.

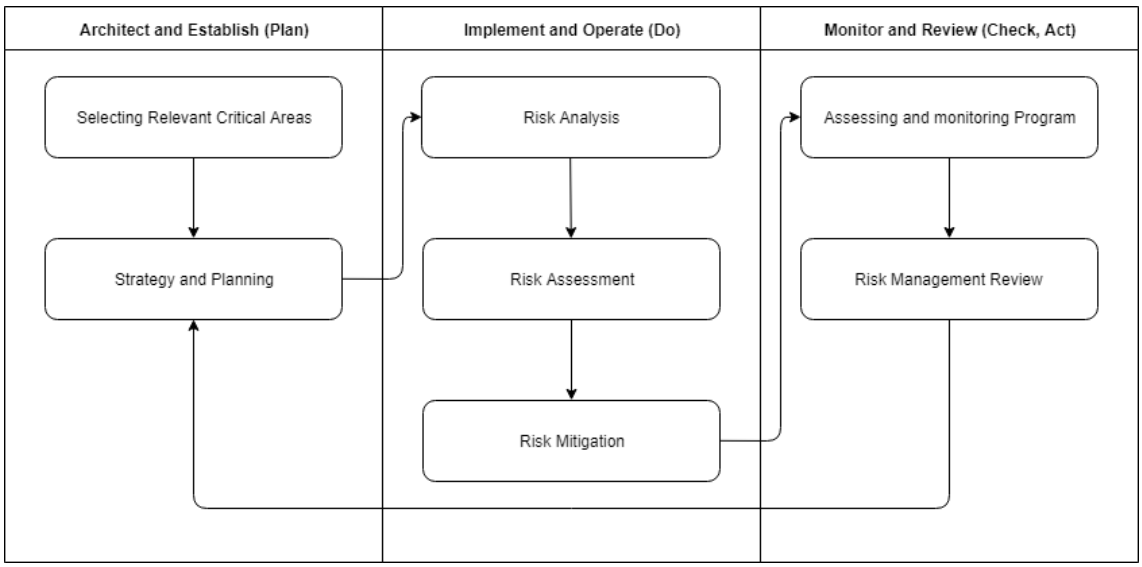

Figure 3. Simplified version of risk management framework for cloud computing (Zhang et al., 2010)

Selecting the relevant critical areas of focus has many domains to consider, while keeping the cloud service and deployment models in mind. As an example, SaaS provider may select application security and access management as key areas. The purpose of strategy and planning is to define goals, requirements and scope for the risk management program, and proactively plan activities to reach set goals and requirements. Risk analysis has much depth and different approaches on how it can be conducted, but in order to be effective, it needs to be part of the business process of the whole organization. In many methodology cases, risk analysis incorporates two interrelated elements: threat identification and vulnerability identification. Risk assessment is the output of the risk analysis and has four key processes: likelihood determination, impact analysis, risk determination, and control recommendations. (Zhang et al., 2010)

Due the multiple different models of cloud computing available, there are various ways to create a risk treatment plan (RTP), which can have multiple options such as avoidance, transfer, retention, reduction and acceptance. This plan can be used to mitigate vulnerabilities or threats. Assessing and monitoring program can be conducted for example through internal audits. Risk management reviews are team meetings and are meant to assist in the development of an approach to loss prevention. (Zhang et al., 2010)

Risk management can also be viewed and discussed from different viewpoint compared to the technical approach. Kayworth & Whitten (2012) proposed three types of risk management mechanisms, deemed critical in effective IS security: organizational integration, social alignment and technical competence.

With organizational integration, most of the security functions are centralized, led by an executive, such as chief information security officer (CISO). This helps to develop and deploy consistent enterprise-wide security policies and standards. The key is that the management can participate in planning processes that are reviewed by top management. This helps to avoid isolation of the technical information security functions. Internal audit groups can help to ensure that information security controls and policies assessment results are relayed to the management. This is backed by Kayworth & Whitten's (2012) interview of one security manager at TechServ: *"A very strong corporate audit function is required to ensure that the operational [controls] are meeting the requirements of the strategy"*. (Kayworth & Whitten, 2012)

Social alignment as risk management mechanism helps to align information security with the business. According to Kayworth & Whitten (2012), there is a need to develop a culture that embraces the value and importance of security within the organization. By promoting cultural awareness, employees will feel more motivated to follow the set security practices and policies willingly, rather than through rough control. Hsu (2009) demonstrated in his study about interpreting implementation of ISS certificates in an organization that by imposing strict compliance procedures at the studied company Finance House, did not guarantee improved security due employee's assumptions and individual interpretation of the relevance of security management. Some employees were found neglecting compliance due convenience reasons.

The social alignment can be achieved by executive commitment, security awareness programs, informal networks, and with information security mentoring. Executive commitment means that management actively participates and supports information security as a meaningful enterprise-wide function. Security awareness programs are training and education, provided by the company to the employees. Informal networks cover internal and external stakeholders that engage in security, e.g. IT audits and security vendors. Information security mentoring is informal consulting and advisory to other parts of the company. Its purpose is to create better security awareness throughout the organization and lower the bar to seek advice on security-related issues. (Kayworth & Whitten, 2012)

It can also be argued, that there is no single technology or mechanism to ensure success with effective information security. According to Kayworth & Whitten (2012), there is need for application of multiple organizational and social mechanisms, combined with technical competence. This forms a socio-technical strategy, thriving towards effective information security.

Investment decisions

The frequency of security incidents are rising and so are the costs of managing and mitigating security breaches (Shao et al., 2019.). Budgeting for information security expenditures is therefore a crucial task for organizations (Gordon & Loeb, 2006).

According to Shao et al. (2019), the budgeting issue is usually addressed by two different research streams: decision-theoretic approach and by game theory. Decision analysis is a decision-theoretic model, composed of different calculation models used to assess risks (Shao et al., 2019). Most basic one is to compare the risk and return of investments: return on security investment (ROSI). It is derived from classic return on investment, which is an evaluation of investment. ROSI is calculated as follows:

$$\mathrm{ROSI}(\%) = \frac{\mathrm{ALE} * \text{Mitigation ratio} - \text{Cost of solution}}{\text{Cost of solution}} \quad (1)$$

ALE is the annual loss exposure, the total annual monetary loss expected to result from an exposure factor if the security investment is not made. The calculation of ROSI is only an estimate, since it is hard to obtain data about the total cost of a security incident. (Sonnenreich et al., 2006)

There are more complex variations on decision analysis, such as usage of value-at-risk approach, or cost-benefit analysis (Shao et al., 2019). From economics perspective,

Gordon & Loeb (2006) suggest, that one way for organizations to budget their expenditures is through cost-benefit analysis, used with net present value model (NPV). The processes includes estimating and comparing the risk-adjusted discounted present value of expected benefits with expected costs. (Gordon & Loeb, 2006.)

It is however hardly ever possible to use completely rational cost-benefit analysis model in the budgeting process due the nature of the information security investments (Gordon & Loeb, 2006). Shao et al. (2019) also agree that there is uncertainty in information security that hinders the managers' ability to utilize cost-benefit analysis in practice. It is hard for managers to estimate the expected costs of information security investments, since they are unable to get historical data to make predictions. Security investments also have intangible benefits, meaning that estimating the anticipated benefits of an investment requires the managers to have data on potential losses from a breach and the probability of such a breach. Moreover, in many cases there is no way to create reliable actuarial loss statistics in order to predict future benefits. (Shao et al., 2019.)

According to Gordon & Loeb (2006), some of senior information security managers tend to use formal analysis to calculate security expenditures, but others use modified approaches, examining the costs and benefits of security activities with less weight on formal quantifiable benefits. The ability to utilize NPV analysis in budgeting relies on the ability to estimate benefits. It should be noted however, that managers do not need to follow this strict and rational economic route in order to have an economic approach to the issue. Modified economic models can also be used, e.g. considering potential losses from security breaches. (Gordon & Loeb, 2006)

Instead of relying on pure economic calculation like cost-benefit analysis, managers might need to rely on recommendations from experts or follow processes used by other organizations (Shao et al., 2019). In addition, Gordon & Loeb (2006) note, that in their interviews, senior information security managers may also use last year's budget, and best practices in the industry as a factor when doing information security budgeting.

Game theory is an alternative approach alongside decision theory on the ISS investment problem. In this context, game-theoretic approach can be used to "analyze problems in which the payoffs to players depend on the interaction between player's strategies" (Cavusoglu, et al., 2004). In other words, game theory specializes in analyzing the decision-making in an interactive environment and provides the method to achieve optimal configurations and classification strategies (Herbert & Yao, 2008). The players in this case are the hacker and the organization, and the nature of the game played will depend on the timings of hacker's and organizations actions (Cavusoglu et al., 2008).

Two scenarios are differentiated by Cavusoglu et al. (2008): simultaneous game and sequential game. In the simultaneous game, the organization and hacker make investment decisions and effort concurrently. With sequential game, the organization makes the investment decision first, and hacker reacts to this effort after learning it. Cavusoglu et al. (2008) rationalize that the sequential game can be possible in cases where the organization publicly announces about its security investment, for example firewalls or authentication systems. Alternatively, hackers can utilize social engineering and digital probes to determine the protection methods and level in the organization before making their move. The playout of sequential game can be considered rarer, since if the hacker is unable to verify (observe) or does not believe the organizations decisions it has made, the game will revert to simultaneous game. In this mode, each of the players will assume that other changes its strategy based on the other's actions. (Cavusoglu et al., 2008.)

Compared to decision-theoretic approach, game theory seems to yield higher payoff to organization on security investments, especially when sequential game is played where the organization goes first. And if the organization can control the sequence of the actions of the players, it should force the hacker to play the sequential game. If the managers understand the motivation of hackers and the utility they develop, more positive economic outcomes can be achieved than with decision-theoretic way. However, as there can be uncertainty with the game theory's parameters (incomplete information), the payoff edge it provides compared to decision-theoretic approach diminishes as the uncertainty grows. This makes it less attractive choice for organizations, and they may stick with decision analysis model, when budgeting on information security. (Cavusoglu et al., 2008.)

ISS policy development and implementation

Though designing information security policies within an organization may typically fall to the security specialists, it is the managers who implement them and ensure the compliance with them. ISS management standards, such as ISO/IEC 27001, NIST-SP800, and PCI-DSS play a definitive role in the management of ISS. They provide one method of implementing the ISS management and attempt to provide guidelines to best practices in the area. In fact, these and many more standards are made to be a collection of best practices, aiming to be authoritative, general, and detached from actual practice. It is because of their universality and general nature, that the standards provide little practical guidance how organizations adopt them in practice. Standard like ISO/IEC27002 provides implementation guidance for ISO/IEC27001, which requires organizations to establish an ISS policy, but due the high level of guidance organizations can find it challenging to do so. (Niemimaa & Niemimaa, 2017.) For example, Wiander (2007) demonstrated in his study, that the readability of ISO/IEC 17799 certificate was criticized in addition to the implementation process of it, when the studied organization implemented it.

Niemimaa & Niemimaa (2017) found out in their ethnography study, that the target organization did not have much trouble translating the best practices from ISS standards to actual ISS policy but fitting the new policies to existing local work culture and way of working. The key is to implement ISS policy in such a way that it becomes part of existing practices and performable by the employees. Supporting the argument, Wiander (2007) found out in his study that for information security to work properly in an organization, it needs to be implemented in the daily activities of the organization. Understanding it and maintaining continuous support from management is also crucial, mere adaptation of certificates or a security standard does not guarantee adequate information security level. Puhakainen & Siponen (2010) also explain that top management's support is important to ensure employees' compliance with ISS policies.

Kayworth & Whitten (2012) also stress that maintaining cultural fit is important. Security managers and executives need to ensure that the underlying information security value are aligned with the values of the organization. Employees tend to behave in a way corresponding the corporate values. Cultural conflict may occur, if the applied information security program or policy does not match the values of the company. The conflict may show itself as inconsistent behavior or resistance among the individuals with set policies and standards. Similarly, Niemimaa & Niemimaa (2017) implied, that ISS policy should become congruent with the organizational practices.

Niemimaa & Niemimaa (2017) further state in their findings about ISS policy congruency with organizational practices that organizational practice should be allowed to reconstruct

the policy during development and implementation. Authors demonstrated, that organizations canonical practices are not fixed but are continuously produced and reproduced as they are enacted. In practice, this means that the organizations, through their practices, shape the developed ISS policy. This understanding challenges Stahl et al. (2012) implications on policy development and implementation that policies should be imposed, not negotiated with (Niemimaa & Niemimaa, 2017). For example, Stahl et al. (2012) present a mechanism to uphold the ideologies implied in implemented policies preventing them from being questioned: silencing critical voices.

One reason for organizations to adopt standards and best practices, is to comply with different legal and legislative demands (Niemimaa & Niemimaa, 2017). For example, government may require an organization to comply with certain standards in their operation, which is emphasized especially when the organization operates globally. Design and implementation of information security policies need to comply with external legal requirements. This varies by industry, and the geolocation of data the organization stores. (Kayworth & Whitten, 2012.) Another reason for implementing security standards is competitive advantage gains that can be acquired. Wiander (2007) found out through interviews that the motivation for ISO/IEC 17799 certificate implementation in studied organization was to meet client needs and to gain competitive advantage in the industry. The certificate appeared to also support sales efforts and provide a formalized security framework for the organization to follow.

As recommendations how ISS policies should be developed and implemented in practice, Stahl et al. (2012) propose to use accessible language and terminology in order to minimize misunderstandings. The guidelines from the policies should also be separated in such manner, that employees have their own set of employee-oriented guidelines and that specialists have their own technical content in separate documents or as appendices. The policies issues that are relevant to the specific groups should be emphasized and their relevance demonstrated. By different viewpoint, Niemimaa & Niemimaa (2017) suggest that enacting ISS policy requires employees to break their existing habits and reconstruct new non-canonical practices.

2.3.2 Employees: compliance to information security policies

Nowadays, one of the major concerns for security managers, if the employee's non-compliance with organizations ISS policies. The non-compliance can be due to multiple reasons, and multiple behavioral theories have been used to explain and discuss this behavior. Security managers need to make sure that employees follow the set policies.

Employees' failure to comply with security policies is a major concern for security managers (Siponen & Vance, 2010). By estimation, over half of information system security breaches are caused or related to employee's poor ISS compliance (Siponen & Vance, 2010). According to Chen et al., (2012), employees do not always seem to be motivated to follow security policies and instructions set by the company. It is more like they follow their habits and routines and tend to be resistant to behavioral changes. Siponen & Vance (2010) add that employee's violations of ISS are caused most often due the negligence or ignorance of the set ISS policies, even in organizations were security specialists are present. D'Arcy et al., (2014) found evidence in their study about the information security policy violation phenomenon that employees perceive stress due the set security requirements and are more likely to rationalize security policy violations through moral disengagement. This results in increased exposure to violate the set policies. It is recommended, that organizations need to know about and counter security-

related stress (SRS) amongst employees. Security related overload, complexity and uncertainty are factors that signify the possible existence of SRS. (D'Arcy et al., 2014)

There are a multitude of other theories explaining security policy compliance. Moody et al., (2018) review 11 theories (that more or less overlap with each other) and attempt to unify them to explain the compliance issue. Few of these theories are introduced in this study. To understand violations of ISS policies and employee non-compliance, *deterrence theory* is traditionally used (Siponen & Vance, 2010). Its origins are in criminology, explaining criminal behavior. Deterrence theory's main tenet is that individuals (for example employees), engage in crimes when the benefits outweigh the potential costs (Moody et al., 2018). In other words, if the individual thinks that the risk of getting caught is high (certainty of sanctions), and the penalty of the sanctions is also high, according to the deterrence theory, the individual would not commit the crime. Traditionally, formal sanctions are described as deterrent mechanisms for the theory but since the introduction of the theory, it has been extended with informal sanctions such as shame and disapproval from friends or peers. (Siponen & Vance, 2010)

Deterrent strategies are recommended against unwanted behaviors like IS policy non-compliance or computer abuse (Chen et al., 2012). The term computer abuse is in this context comparable to computer misuse (computer abuse is continued to be used further here). Although wide notion, computer abuse is a key source of security incidents, yielding up to 50 to 70 percent of all incidents happening in an organization, causing major financial losses (D'Arcy et al., 2009). Direct punishments have been shown to reduce the abuse intention on employees when the perceived certainty of enforcement and severity of the punishment increase. (Chen et al., 2012)

It should be noted however, that in contrary to other studies, D'Arcy et al., (2014) found no direct relationship between perceived sanctions and information security policy intention when studying the role of sanction in security compliance decisions. Moreover, Abed & Weistroffer (2016) found out in their meta-analysis that formal sanctions have low certainty and celerity on individual's compliance intentions. Abed & Weistroffer (2016) used certainty and celerity as deterrence constructs and inspect their correlation to compliance intention. They also noticed, that certainty has more influence on employee's compliance than severity.

In their study, Siponen & Vance (2010) also argue based on prior research on Criminology, that employee's violation of ISS policies is not best explained by the fear of sanctions, namely deterrence theory, because employees may utilize neutralization techniques or rationalizations, which minimizes the perceived harm of those violations. *Neutralization theory*, as first introduced by Sykes & Matza in 1957, suggests that both law-abiding citizen and those who commit crimes or break rules believe in norms and values of the community. Those who break the rules or commit crimes apply techniques of neutralization to render the existing norms, rules, morality, and obligations to law temporarily inoperative by justifying their behavior. As an example, person breaking organization's security policies justifies his actions in the moment by claiming (to oneself) that no actual harm will be done. This way the person avoid guilt by reasoning that there is no criminal or rule breaking behavior involved. By neutralizing behavior, person can maintain their noncriminal image and slide back and forth between what is considered being law-abiding or criminal behavior. In theory, because neutralization techniques exist, it gives and explanation why sanctions may lose their effect in some cases. (Siponen & Vance, 2010; D'Arcy et al., 2014)

Different neutralization techniques have been proposed over decades in addition to the original formulation of five techniques by Sykes & Matza (1957). Siponen & Vance (2010) presented and explained six of them in their study: denial of responsibility, denial of injury, defense of necessity, condemnation of the condemners, appeal to higher loyalties, and the metaphor of the ledger. With focus on compliance with organization's security policies, silver bullet is hard to point out, which technique explains it the best, but according to Siponen & Vance (2010), neutralization is an important factor to consider when developing and deploying security policies and practices within organization. In addition to Siponen & Vance (2010), D'Arcy et al., (2014), Barlow et al., (2013) and Teh et al., (2015) have also used neutralization techniques before to explain employee non-compliance with ISS policies within organizations.

Rational choice theory (RCT) is similar to deterrence theory. It assumes that criminal individuals are rational, calculating and weight the perceived benefits and costs of engaging in the criminal act and the chance of getting detected. Like with deterrence theory, RCT also contains formal and informal sanctions, but its models also have benefits as rewards. The sanctions are regarded as costs. These include the negative outcomes of the chosen action or behavior. To apply the theory, it is assumed that costs have severity and susceptibility component which are needed to invoke the perceived threat by the individual. (Moody et al., 2018; Siponen & Vance, 2010)

Protection motivation theory (PMT), founded by R.W Rogers in 1975, deals with fears. PMT explains how individuals are motivated to react to warnings about threats or dangers and how their behaviors are elicited as a response to a fear appeal. PMT does not assume that the choices of the individuals are rational, the assumption lies in that the individual is responding to the fear appeal. Severity and susceptibility of the threat are again needed in order to evoke the perceived threat in the individual. Vance et al. (2012) explain, that PMT suggest that information about a threat triggers a cognitive mediating process. This process includes threat- and coping appraisal responses. With the theory application in ISS policies, employee's non-compliance to these represents a maladaptive response and compliance with the policies an adaptive response (Vance et al., 2012). The maladaptive response invokes the treat appraisal factors, such as vulnerability, perceived severity and rewards. This reduces the probability of maladaptive response, like non-compliance towards ISS policies. (Vance et al., 2012; Moody et al., 2018)

These theories can help to explain the behavioral reasons on employee's non-compliance. They can also help to understand, what effective ways to counter it are. Alternative strategy to punishment or sanctions are rewards. Employees have been shown to think that set policies and procedures are not mandatory and therefore may not always comply with them. They may not also interpret them correctly or adhere to them over time after the policies are set. Setting up rewards can send a strong signal, that complying with ISS policies is mandatory. Rewards and other benefits are also influencing factor when employees make a rational choice of compliance or other way. (Chen et al., 2012.)

The common ways to enforce compliance that organizations use are coercive, remunerative and normative control mechanisms. Coercive control uses threats and punishments to regulate non-compliance. Remunerative refers to economic incentives that organization may use, e.g. bonuses, commissions or promotions in exchange of compliance. Normative control approach relies on moral reasoning and the values of compliance are heightened. (Chen et al., 2012.)

However, as a different opinion Karjalainen (2011) suggests that using these theories in the context of ISS compliance can also be viewed as too generic and perhaps not

completely applicable in in this specific context, since they sprout from different fields of study. There is a need to explore, grounded in data, why and how employees comply or do not with ISS processes and policies in order to improve the compliance of ISS policies.

ISS Training to address the issue of compliance

To address the problem of employees failing to comply with ISS procedures and causing harm to the organization, different methods have been proposed in literature: use of sanctions and deterrence's, marketing campaigns, and training (Karjalainen, 2011). It can be argued that training employees and other stakeholders for new ISS policies, security measures or technologies is an important task in order to achieve and maintain effective IS security within an organization. In fact, training is most commonly suggested in literature to address IS policy compliance (Puhakainen & Siponen, 2010). For larger organizations, this training typically falls to IT security specialists.

ISS training differs from traditional training that employees might encounter. It is non-cognitive and persuasive in nature, emphasizes on daily work situations, and incorporates the intangible nature of the information security threats and assets (Karjalainen, 2011). There are different paradigms to discuss effective ISS training, such as behaviorism, cognitivism, constructivism, and learning.

Hsu (2009) explains that existing ISS literature recognizes the importance of the design of training programs and education in order to enhance employees' awareness. However, his findings imply that the education and training that took place at Finance House when adopting new certificate, had no real effect on employees and seemed ineffective. The employees retained their existing beliefs on IS security and did not adopt new processes insisted in the BS 7799 Part 2 certification that the case company implemented. Hsu (2009) discusses, that it might have been more important to focus on bringing about attitude and belief changes in order to achieve lasting changes in security behavior within the employees. Furthermore, Hsu (2009) suggests that in order to increase security awareness throughout the organization, frames analysis could help IS security specialists and managers to identify negligence of IS security in early stages and draw an intervention strategy to counter it. Frames analysis concept is believed to provide a tool for understanding behavior and perceptions of related social groups when new ISS policies or other ISS practices are developed and implemented in an organization. The outcome of the analysis can be further processed to develop effective training strategies.

Puhakainen & Siponen, 2010 argue that IS security training programs should also provide a theoretical explanation *why* they work, in addition to the empirical evidence *that* it works. In other words, Puhakainen & Siponen (2010) suggest that that good and effective training program in IS security is both empirically and theoretically grounded. If the training program does not work in practice, it is of little use. On the other hand, if the practitioner does not understand the underlying theory why it works, the application my fail in different situations and the practitioner will not know why. According to Puhakainen & Siponen (2010), previous studies regarding IS security training have little empirical evidence of their usefulness in practice.

In their action research study Puhakainen & Siponen (2010) presented a new ISS policy compliance training program, based on universal constructive instructional theory (UCIT) and elaboration likelihood model (ELM). The UCIT helps to create a concrete framework for situated training, customizing the certain learning subject and target group of the

training. ELM explains how expected and enduring behavioral changes can be achieved through cognitive processing. It can also help to understand how and why training is likely to work. (Puhakainen & Siponen, 2010.)

Key findings from Puhakainen & Siponen (2010) implicate that a successful ISS policy compliance training should take into account the target's (e.g. employee) previous knowledge on the subject. The training programs should also be tailored to be relevant to the learner, meaning that it should relate to the actual work the learner is doing in the organization. To improve the motivation for the employees to comply with set policies, the ISS training should be integrated in with normal business communication of the organization. Moreover, the training carried out in the organization should be continuous activity instead of one-time session, to increase compliance further. (Puhakainen & Siponen, 2010.)

2.3.3 IT security specialists

IT security specialists (or ISS specialists), traditionally work with corporate security, being responsible of managing ISS within the company and ensuring the continuity of business. One job function can be for example incident response, risk analysis or policy development. Specialists can also be responsible of selecting security technologies for the organization, or training employees for new security measures or policies. More likely actor to actually select security technology for the company is the management, but since there is multitude of things to consider in the selection process, the specialists will most likely be more involved in the process.

Selecting security technologies

As mentioned before, sometimes organizations may also choose to adopt the security technologies used by other organizations and follow their practices. Related to this is the *herding behavior* that individuals tend to express when facing difficult decision and when posing limited ability to predict the value of a security investment. This is common due the uncertainty that is attached to ISS. State-, effect- and response uncertainty all describe the struggle in precisely predicting the outcomes of adaptation of new security technologies. State uncertainty refers to the lack of confidence the involved person has in his ability to predict what the major events or trends in the environment are or how they will change. Effect uncertainty means that the person cannot predict the effects that the changing environment will do to the organization. Response uncertainty is the inability to predict the possible consequences of a response choice. For example, predicting how effective a security technology investment is when deployed. (Shao et al., 2019)

Herding behavior is also influenced by the reputation. It is associated with performance evaluations, promotions and compensation. Since the uncertainty factor shrouds the evaluation of profitability in the investments, especially managers who have good reputations and are uncertain about the outcomes of an investment, tend to make decisions based on others, to maintain the reputation. Good reputation means that e.g. carried out investments were profitable. (Shao et al., 2019)

There are also more analytical ways to select security technologies. Strategic investment decision on security technologies can be done for example using game theory or by economic calculations as introduced earlier. Related to it is selecting the right security technology to be used within the organization (companywide or as a local solution). There

are many stakeholders involved in this process, e.g. managers, investment board, acquisition team and others (Radack, 2004). More directed tasks related to IT security specialists concerning the selection of security technologies for organization comes from, comparing costs and features of different solutions and reviewing the compatibility with existing systems. Radack (2004) also list other product considerations that organizations should take into account relating to the selection process: total life cycle costs, ease of use, scalability, and product vulnerabilities. Equal importance is also to review lists of validated products, for example by National institute of standards and technology (NIST).

Chou et al., (2006) proposed a fuzzy multi-criteria decision model (FMCDM) to help stakeholders to evaluate potential new investments. Simplified, it has two stage evaluation processes, including 26 criteria for the target investments. Each of the criteria is given a relative weight using linguistic values. This model shows many factors that affect the decision of selecting the best candidate solution from a selection of many. The case study Chou et al., (2006) conducted, showed that different stakeholders had different ideas of most important criteria when the model was used. Focusing on the IT staff, most important factors were compatibility or ability to integrate with existing IT/IS portfolio, manpower, and probability of benefit achievement.

Tang & Liu (2015) inspected in their case study SaaS cloud model transition and selecting cloud service provider (CSP) partner for organizations. Their findings also discuss the importance of interoperability, security governance and legislative concerns. Understanding the connection with cloud computing and the regulatory environment is important, and how the data organization stores is subjected to it. Relating to governance, there should be agreement with the CSP about termination conditions and costs (cost of switching), data extraction, data migration and disposal. Regarding the interoperability, there might be a problem if organization decides to change CSP, and the data is in such format that it is impossible to be migrated to different cloud platform, effectively causing vendor lock down. Interoperability should allow ease movement of data and applications from platform to platform.

The phenomenon of chasing the hottest IT

When new information technology emerges, a question often rises inside an organization: is this the next big thing or a passing whim? This means is the new promising technology such an innovation that it will be widely adopted by many organizations and institutionalized, or will it soon be abandoned and forgotten (Wang, 2010). The term IT fashion is, as Fichman (2004) defines it: “a transitory collective belief that an information technology is new, efficient, and at the forefront of practice”. IT fashion is named as such, because technology can be described like in terms of ‘fashion’. Some new technologies are long lived, and they provide lasting utility, some are only useful for limited time or provide only minor benefits. All of these are subjective to the swings of fashion. (Wang, 2010.)

When organizations engage in IT fashion, they engage in innovations. An organizational innovation is as Wang (2010) describes it, a structure, practice or technology that is new to the organization adopting it. Closely related to all this is Roger’s 1962 diffusion of innovations theory, which states that innovations gradually spread amongst organizations (Rogers, 2003).

Wang (2010) argues that IT fashion influences organizations performance, reputation and executive compensation. Furthermore, following fashion can legitimize organizations

regardless of their performance when reflected on middle phase of diffusion of IT innovations. Based on institutional theory, organizational legitimacy is often chased by adopting practices and innovations that are established and already used by other organizations. As an example, one way for organization to gain legitimacy is to inform their stakeholders about involvement in socially accepted IT.

When an organization invests in IT innovations that are in fashion, they may expect lower initial performance for couple of years, when afterwards performance gains can be expected. As an example, investing in new ERP system may cause initial performance dip due the new required processes that disrupt the current workflow. Organizations reputation can also be affected by following IT fashion. Wang (2010) showed in his study that companies are considered more reputable when they are linked to and invest in IT innovations that are in fashion, regardless of the performance lags for the first years of implementation. Additionally, organizational leaders can expect higher compensations when following IT fashions in forms of bonuses or higher salary, again regardless of the initial performance impact on the business. (Wang, 2010)

3. Methodology

In this chapter, qualitative research methods are introduced, with focus on case study research method and the reasons for selecting it for this study in context of information systems. Moreover, the data collection method is explained and the analysis of the collected data from the case organization.

3.1 Qualitative research

Qualitative research has its roots in social sciences and were originally developed to study the social and cultural phenomena. “In qualitative methodology the researcher looks at settings and people holistically; people, settings or groups are not reduced to variables, but are viewed as a whole.” (Taylor et al., 2015)

Ketokivi & Choi (2014) describe that qualitative research examines concepts in terms of their meaning and interpretation in specific contexts of inquiry. Seaman (1999) thinks qualitative data as words and pictures, excluding numbers which can be considered to be part of quantitative data. He reasons that qualitative research methods were designed to study human behavior and complexity of it. This is because many other phenomena can be explained and presented by other means, for example numbers and statistics. Seaman (1999) also reasons, that especially in software engineering, usage of qualitative methods forces the researcher to think more deeply on the subject and not abstract it away. This can yield more informative and richer study than with the usage of only quantitative research.

This considered, the difference between qualitative and quantitative methods are that data is quantitative when it is numerical, for example measurements. This can be collected for example through polls or questionnaires. Qualitative research as Seaman (1999) explains, focuses on human aspect and tries to give insight on the underlying reasons and motivation. Myers (2013) also concurs, that qualitative researchers in general argue that in order to best understand people’s motivations, reasons, actions and the context of their beliefs in depth, qualitative research can be appropriate.

Pettigrew (2013) also adds that qualitative methods are powerful in observing people’s everyday lives through frameworks, since it is linked to people’s social processes. In his study Pettigrew (2013) also refers to prior work on qualitative research in organizational setting and based on that argues, that best qualitative work is contextually grounded and aims to explain process dynamics and not just the outcomes.

Qualitative research methods were developed in social sciences to help researchers to study the social and cultural aspects and phenomena. The key benefit of qualitative research is that it enables researcher to understand the context where actions and decisions take place. Sometimes it is the requirement to see and understand the context in order to understand why something happened and why some did something that way. It is virtually impossible to understand why or how something has happened without talking to people. (Myers, 2013) If we reduce people’s words to statistical equations, we can lose the sight of the human side and its effect on inspected subject. Since this thesis focuses on the human factors rather than technical aspects in cloud security, qualitative methods or rather case study, is the chosen approach. (Taylor et al., 2015)

It is also important to understand the underlying philosophical assumptions that guide the research and make it valid (Myers, 2013). These reside behind all research approaches, whether quantitative, qualitative or design science. Some of the assumptions relate to the underlying epistemology that influences the chosen research approach. Epistemology in this respect relates to the assumptions about knowledge and how it is attained. These epistemologies or 'paradigms' they are sometimes called, can be categorized in multiple ways, depending on the researcher and perspective. Myers 2013 splits them into three classes: positivist, interpretive, and critical.

Positivist researcher typically formulates propositions that inspects the subject in terms of independent- and dependent variables and the relationships between them (Myers, 2013). There is therefore a tendency for positivist research to utilize quantitative methods. But as Orlikowski and Baroudi (1991) state in their paper about research approaches and assumptions, a study can be classified as positivist in IS research when there is evidence of formal propositions, quantifiable measure of variables, or hypotheses testing. Positivist stance can therefore utilize qualitative methods such as case study as the way of approach. In fact, case study can be any of the introduced paradigms.

Interpretive research attempts to understand the observed phenomena through the meanings that people assign to them. There are no predefined independent or dependent variables, and the focus is aimed towards the social constructions such as language, consciousness, and shared meanings. Context here is the key, since it defines the situation and makes it what it is. (Myers, 2013)

Critical research is similar to interpretive in multiple ways. The key difference is that critical researcher challenges the current knowledge, beliefs, values and assumptions in contrast to interpretive researcher who just describes the current situation and its nature. Critical researcher can then also suggest improvements to the observed social situation, although the amount can heavily vary. (Myers, 2013)

In this study, a positivist tradition is followed. Unlike in traditional manner, no hypotheses were formed in advance to be tested but the output of the thesis provides clear propositions that can be further tested or identified in other cases as well.

Case study

This study utilizes case study as the chosen qualitative research approach. Motivation for choosing this comes from the qualitative research's ability to help researchers better understand people and the social and cultural context associated with them. Benbasat et al., (1987) think case study as an intensive investigation of a phenomenon in its natural context that may and in many cases involves multiple sources of data.

As already stated, since the purpose of the thesis is to gain a holistic picture on information security management, emphasizing on the associated human factors, case study is a better fit opposed to any quantitative methods. There is no exploratory side as such, since there is prior research on the covered topics and issues relating to the human aspect of the cloud information security.

The advantages of using case study includes what Myers (2013) calls 'face validity'. Well executed case study tells a real-life story about an issue in its natural environment. Case study also allows the research to test theories in specific real-life context where there is infinite amount of (more or less important) variables. Since the real-life contexts are messier than theory is, there can be multiple correct interpretations of the same situation

(Myers, 2013). Case studies also help to answer the 'how' and 'why' questions, to understand the nature and complexity of the processes (Benbasat et al., 1987).

Case research also has its own weaknesses and pitfalls. One problem is that case study findings and results in IS field are not readily generalizable to other settings due to the small-*N* problem (Tsang, 2014). For this study, this is one of the limitations, because making a sound generalization would require more case companies and participants. This paper only analyzes one case company to answer the proposed research questions. Second disadvantage of case study research is the fact that it can be hard to gain direct access to the subject of study; organization or groups of people (Myers, 2013). This issue was countered in this thesis by using contact within the case organization, who was able to email all the groups of interest. Other problems with case studies are the fact that they are time consuming for the empirical part, and also that it can be difficult. The context can be small or large depending on the researcher, and it is important to know what of the data is relevant and what is not. Limitations for the research scope were set right from the start, in order to prevent irrelevant data gathering and focusing on quality and richness of what is collected.

The studied case organization can be categorized as global, multinational, 'large' and operates in the ICT field, specializing in telecommunications. Branching in different markets and incorporating cloud technologies as well as traditional computing in its operations, making it one of the best candidates for a study of this kind.

3.2 Data collection

Seaman (1999) presents two different data collection methods that can be used with qualitative research: participant observation and interviewing. These can be useful when collecting information in IS research. There are many types of interviews but Myers & Newman (2007) differentiate three most common ones as: structured interview, unstructured or semi-structured, and group interview. In structured interview, a ready script is prepared, and there is no room for improvisation. These kinds of interviews tend to be used in surveys. Considering the research topic of this study, structured interview is not the best approach, since restricting the answers of the interviewees too much could hinder the fullness of the answers.

For this study, semi-structured interviewing was chosen as it is flexible and keeps the interview questions somewhat open for discussion, in order to hopefully get more in-depth and richer answers from the participants. It also gives the interviewer the ability to improvise and ask follow-up questions.

Myers & Newman (2007) point out in their paper, that interviews can go wrong. For example, the interviewer can unintentionally offend or insult the interviewee, but the more likely pitfall is the ambiguity of language. It is possible that the interviewee misunderstands the question, and it isn't always obvious when this happens. For this study, this was considered in multiple ways. First, the interview is semi-structured, giving the interviewer flexibility to explain the questions and context in more detail. Second, the interview was conducted in the native language of the interviewees and the interviewer.

Other important problem with interviews that Myers & Newman (2007) mention, is elite bias. This means that the interviewer may interview only selected informants of the organization and fail to acquire understanding or opinion of the broader situation. In other words, interviewing only selected group of people should be avoided since it can give an

incomplete presentation of view in the organization. This was hard to avoid when selecting the interviewees, but the actors and viewpoints (employee, IT specialist, manager) were constructed specifically to counter this. The employees were selected from different teams in the same department.

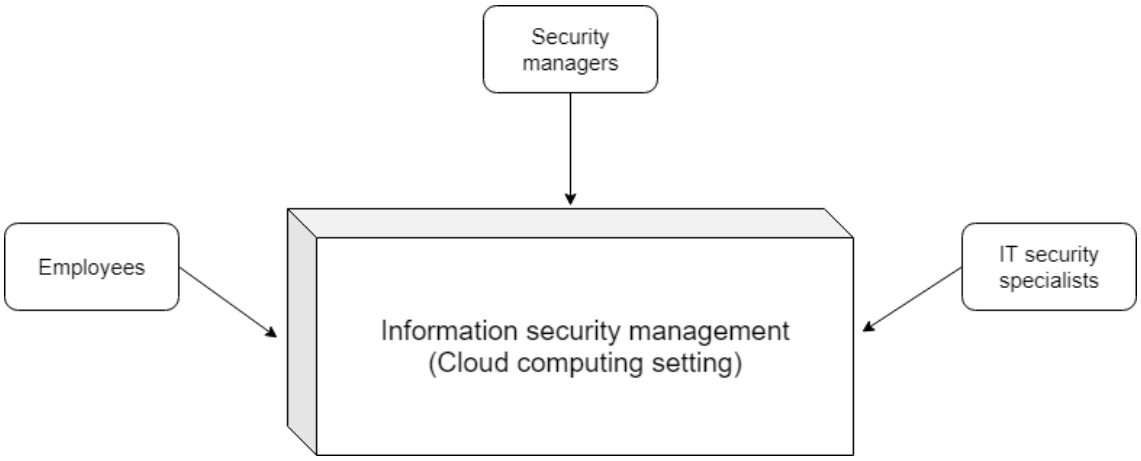

Figure 4. Visualization of the empirical data provided by the different perspectives

The interviewees are grouped in three different actor categories: employees, IT security specialists, and security managers. The interview questions are based on the perspectives and relations that each of these actors have on information security management in cloud computing setting: e.g. employees' compliance and training, IT security specialist's implementation of security technologies, and security managers risk management, policy making and security investment decisions (see Figure 4). In other words, these three angles or perspectives are considered, in order to gain insight on the research issue. Each of the actors have their own related issues and corresponding questions. Taylor et al., (2015) discuss in their book that for the qualitative researcher, all perspectives are worthy of study. This is in counter to Howard Becker's (1967) argument who suggested the hierarchy of credibility, as in that the perspectives of more powerful people are more valid than those of less power. So, in order to gain as good understanding as possible to the research problem at hand, the interviewees have very different positions within the target organization. As an example, both of the manager represent different department within the same company, so their perspective naturally differs although they are asked mostly identical questions.

The interview questions (see Appendix A) were drafted in iterations, with greater focus on the security managers, meaning that few revisions of the question set was done before all of the interview were started. The order of all the conducted interviews flowed from the employees to security specialists and finally to security managers. All of the interviews followed the structure planned beforehand, where the interviewer first introduced the topic of the study and the specific emphasis on the cloud security. Then followed asking the background information from each interviewee and finally moving on to the interview questions. For some of the interviews, the order of the questions was slightly changed during the interview due to direction the interview was going and how familiar the interviewee was with discussed topics.

All of the questions were first drafted in English, then translated to Finnish (see Appendix B), because all the interviews were conducted in Finnish. This helped to get more rich answers from the interviewees due to their native language. Afterwards all the interview data was transcribed from recordings and translated back to English. With total of nine interviews, seven of which were conducted face-to-face in Oulu area and two via phone

call due the geographical location of those interviewees. The interviewees were selected with the help of the organization's line manager and through mass email, explaining the nature of this study and information about the actual session.

Table 1. Summary of the interview

Actor	*Abbreviation*	*Job title*	*Time in current organization*	*Interview length (min:sec)*
Employee 1	Employee#1	Software engineer	20 years	16:02
Employee 2	Employee#2	Software engineer	13 years	11:52
Employee 3	Employee#3	Software engineer	14 years	18:28
Employee 4	Employee#4	Software engineer	20 years	11:43
Security specialist 1	Specialist#1	Security analyst	20 years	21:42
Security specialist 2	Specialist#2	Network engineer	17 years	17:36
Security specialist 3	Specialist#3	Cyber security specialist	20 years	6:40
Security manager 1	Manager#1	Information security manager	3 years	27:46
Security manager 2	Manager#2	Information security manager	20 years	43:35

Actors are given abbreviation and index numbers to differentiate them in findings and discussion chapters (see Table 1). All the interviews were voice recorded with interviewee's permission for the transcribing process. This helped to keep the interview session more natural since there was no need for the interviewer to stop and write. It also aided to avoid misconceptions that might have occurred if the interview was transcribed on the fly. Although the transcriptions were not validated by the interviewees for misconceptions, careful time spent with the transcription and translation process should yield a valid opinion what the interviewees meant. Due the nature of semi-structured interviewing, the question set varies between the same actor groups, also contributing to the variations in interview length (see Table 1).

3.3 Analysis of the interviews

Analyzing qualitative data differs from analyzing quantitative data. Contrary to some conceptions, qualitative research can produce large amounts of textual data, in forms of transcripts and observational field notes. Systematic and rigorous preparation and analysis of the collected data can be time consuming and labor intensive. In addition, high quality analysis of the qualitative data is dependent on the skills, vision and integrity of

the researcher. Nevertheless, when done properly, qualitative analysis can reflect some of the truth of a phenomenon by reference to systematically gathered data. (Pope et al., 2006)

Pope et al., (2006) also mention that software packages can help with data analysis but should not be viewed as a shortcuts to rigorous and systematic analysis. In this thesis, no software was used to process the transcripts.

The analysis in this thesis was conducted to answer the research question of "What are the factors that should be considered in order to improve information security in cloud computing?" In order to answer this, supporting research questions were required. The output of the interviews (voice recordings) are transcribed and translated before presentation and interpretation, attempting to answer the presented problem. No other material beside the interview data were used in the coding process.

The findings are presented mainly by structure formulated in the interviews. However, they closely follow the order of the supporting research questions. The change in themes compared to the original order of research questions is twofold. First, the supporting research questions needed to be limited for such a horizontal study. The other reason is how the empirical data revealed connections and interleaving elements, e.g. how investments, technology and human factors are triangulated. This follows the analysis strategy of deduction.

4. Findings

This chapter illustrates the key findings from the interviews. The three actor's (employees, IT specialists, and security managers) opinions are divided across the topics discussed in this thesis. Again, both managers come from a different department within the same case company, having therefore different perspectives to the discussed issues and topics. The case company operates in the ICT field and specializes in telecommunications. The interviews however focuses in the organization's cloud security, not on the products or services the company offers.

4.1 Risk management

The managers were also inquired, what in their opinion are the obstacles they face when doing information security management. Manager#2 brought up cost barriers:

> *"Cost saving goals often prevent some implementations. There is no 100% security management, it is about minimizing risks. There is always a residual risk left to be accepted. Other considerations are the availability of competitive staff at this time. In this area, I think there is a shortage on the staff side."* (Manager#2)

As for manager#1, he brought up change management as the biggest issue, followed by regulations. As with other companies, significant changes such as addition of new tools and cloud services are continuously made. To coordinate the changes without making any fundamental mistakes in information processing is a challenge, according to manager#1. Concerning the regulations that are applied in the world, manager#1 considers from a security point of view that it is a good thing to be regulated. Though there are big contradictions between countries with regulations and how everything should work.

Risk identification

Risk management incorporates *risk identification,* and both managers were asked how they identify security risks. Manager#1 explained, that they have a formal program for that: critical information protection (CIP).

> "*This will identify what are the company's most critical data resources, including customer information. Based on that, we start to map out how it is used, where it is used, which stakeholders use it, and what are the risks to these. For example, when talking about a R&D system that includes subcontractors, then the risks of these subcontractors should also be mapped. So, we have our own formal methodology within the company how to conduct risk analysis."* (Manager#1)

Manager#2 adds that the company identifies risks every year through the risk management process. Risks are classified according to their value; main risks are listed, and strategic plans are made.

The interviewer asked, can one get accurate number on the possibility of the risks? Both managers agreed that it is very difficult to quantify the probability of the risk with percentage accuracy and its cost implications. As an example, the loss of documents to competitors is much more difficult to count than the cost effects of someone stealing a

physical device. Manager#1 however also added, that the company has different levels of risk probability that can be utilized, for example high, medium and low. Manager#2 explained that the company is working with ISF, where they take some guidance on how to calculate the risks. Manager#2 listed, that they use at least the following models and calculations:

1. Probability per year
2. Medium primary loss (productivity loss) is used to calculate risk values
3. Medium secondary risk (reputation, legal, competitive loss) is used to calculate risk values
4. Inherent risk (probability * loss)
5. Monte Carlo simulation (risk calculation)
6. The probable value of the risk
7. How much does it cost to control the risk?
8. How much remains uncontrolled? (residual risk)
9. Return on control calculation (whether control investments were enough to mitigate the risk)

Manager#2 further elaborated, that the calculation of risks is an important part of the overall risk management. Risks need to be identified and controls established for them. The functionality of the controls also need to be checked.

Risk assessment

Risk assessment was a subtopic security specialists and managers both discussed. Specialist#2 stated that he personally did risk assessment in his current assignment. More precisely, specialist#2 did vulnerability scanning, risk analyzing of a sort. He further explained that all of the lab networks 10,000 unique IP-addresses are scanned quarterly and checked for vulnerabilities, which are patched according to the severity of the vulnerabilities.

Manager#1 explained that the company has different risk assessment levels in use when talking about cloud services and outsourced services. Depending on what is being purchased, three level model is utilized. First, requirements are formulated and how strict they are before presenting them to the supplier of the cloud service. It starts with basic supplier screening, where basic information about the supplier is processed. This is followed by technical inspections, sometimes for example on-site audits. The purpose of the audits is to check that everything is as claimed to be. This process is dependent on the sensitivity of the issue and service being purchased.

Assessing the impact of the risks was subject asked from the managers. Manager#2 categorized risks to primary and secondary. Primary risks are what directly affects production, and secondary risks that affect sales indirectly (primary and secondary loss). Manager#1 explained the company uses incident management process in order to react to incidents. When incident happens, its nature must first be clear and then analyzed. One part of the analysis is to assess the impact of the incident on the company. As an example, cost effects or negative effects on customer relationships. All these are handled through the incident management and the information obtained is later used when doing risk calculations. (Manager#1)

Interviewer asked the managers about risk metrics used in the company, where manager#1 continued to explain the risk assessment process:

> *"...we follow a multi-stage process for risk analysis of critical information systems. We look what the risks are, go through them, how they should be mitigated and what can be accepted as such. We actively monitor the mitigation status, the extent to which there are open risks that could affect the critical data sources and the schedule they should be closed down."* (Manager#1)

Specialist#1 further widened the view on risk assessment conducted in the case organization. He explained, that they go through risks keeping in mind what are the vendor's abilities (cloud solutions) to act according to company's wishes. Then evaluation is done, are there any login risks, technology risks, or risks to meet the requirements of the company and at what level (not at all, in part etc.).

Residual risk was also covered in the interviews. Interviewer asked the managers, is there a possibility that residual risk can result in huge loss for the company? Manager#2 responded that the purpose is not. Residual risk must be such that it does not cause large losses. Manager#1 explained the procedure related to residual risk. When doing risk mitigation and left-over residual risk is still significant, a decision is required if more mitigation needs to be done or will the matter be taken to upper management to be signed that the residual risk is understood and accepted. There is therefore a formal risk acceptance process within the company if the residual risks remain significant after mitigation. (Manager#1)

Overlooking of risks is also possibility when doing risk assessment. Manager#1 revealed that this issue is present regardless of risk methodology used. Manager#2 also thought it to be possible, although no such incident has yet happened.

4.2 Security technology selection

Both security specialists and managers were interviewed with questions relating to selection of security technologies and investment decision making. The specialists were asked what things they consider when they select security technology for their company. Each of the interviewees had different tasks within the company and therefore different perspectives. Specialist#1 listed interoperation and integration with other security systems and joint manageability (overview of the systems from one place) as most important factors. Specialist#2 thought on the question in more general manner:

> *"Nowadays it is recommended to implement a generally adopted existing security baseline. It can be dependent on a standard, for example ISO-27001, or something that is based on ISC checklists, found on the internet. These can be utilized for example when setting up a firewall or a cloud service. I would start with these and look for the basics, what are the most widely and commonly accepted specifications. Then take the costs and usability in consideration."* (Specialist#2)

Both managers were also asked about the selection process of cloud security technology and asked for an example. Manager#2 noted, that at baseline, security of cloud services in cloud environments are pretty non-existent as of now. The add-ons that are offered, need to be paid separately.

> *"When dealing with users' personal data, the geolocation of the services that we are investing becomes important. Nowadays there are many restrictions what information can be exported to each country."* (Manager#1)

Manager#1 also stressed that the backgrounds of the vendor they are purchasing from is important: whether their technical solutions are scalable, whether they have operated in the market for a long time and are their solutions compatible with existing systems within the company.

Table 2. Summary of considerations in cloud computing technology selection

Factor	***Interview source (Actor)***	***Description***
Usage of standards as a security baseline	Specialist#2	*Generally adopted existing security baseline / most commonly accepted specifications in the industry. Usage of e.g. ISC checklists, or ISO-27001 standards*
Interoperation and integration	Specialist#1, #2 Manager#2	*Cloud service interoperation with other/older systems and integration with existing systems*
Joint manageability	Specialist#1	*As much as possible should be viewed and managed from one place*
Cost effectiveness	Manager#1, #2, Specialist#1	*Cloud investments are considered as operational expenses (Opex)*
Vendor lock-in	Manager#1	*Customer being unable to switch vendors without substantial switching costs*
Vendor reputation	Manager#1	*How long has the vendor operated in the market? What are their past security incidents?*
Scalability of solutions	Manager#1	*E.g. load scalability or functional scalability*
Geolocation of the services	Manager#1	*There are many restrictions on what information can be exported to each country*

It is important to note how cloud security strategy differs from on-premises security strategy. Specialists and managers were asked about this and while the contents of the answers were once again dependent on the perspective the actor had on the subject, common theme circled around investments and costs. When comparing cloud security strategy and on-premises security strategy, according to manager#1, investments are targeted differently. Traditional online model (on-premises security) is associated with

capital expenditures (Capex), such as firewalls and internal network investments, while cloud services can be considered as operational expenses (Opex) when solutions are bought as a service from a partner. This emphasizes the reliability of this partner or contractor (see Table 2). Manager#1 also stated that no vendor lock-in should be allowed. If some cloud service is taken into use and data stored into it, a situation where something happens and as a result data could not be extracted from the service would be detrimental to the operations. API's need to be relatively open, to allow the stored data to be extracted from the service in any situation.

Chasing the hottest IT

When interviewees were asked on what ways' security investments can be made, there was no indication that the case company attempted to be first adopters on cutting edge innovation and reverted back on more calculating approach and well understood and sound technology investments. As an exception, when specialist#3 was asked what things he needs to consider when selecting security technology for the company, he answered that the company is adopting new end point detection and response (EDR) system in near future. The technology is still an emerging field, but there are existing solutions and vendor offerings that companies can already implement.

Therefore, since there was no specific mentioning on being early adopter or investing in something that is considered 'being in fashion' right now, no assumption can be drawn from such limited amount of information. Interviewees were no specifically asked about the phenomenon of chasing the hottest it or about IT fashion.

4.3 Security investments

Security investments

As already stated, costs are a repeating factor that is attached to security technology selection and investments. Manager#1 explained that costs need to be in line with functionality that the investment provides. Manager#2 also concurred, that most important vectors in security investments are how many risks can be managed with as little investment as possible. In other words, the magnitude of the risk, its criticality, and how much it can be minimized versus the investments against it.

Specialist#2 explained his thoughts when asked about what factors affect possible security investments:

> *"When working in a company which purpose is to make money for its owners, every matter will be calculated as a business case. The money decides what sort of a solution is bought. Every possible information security risk has to be turned into a monetary value, which of course is always just an estimate. You have to be able to point out that the security solution is a positive business case, no matter how great it would technically be."*

It also became clear, that one of the hardest things with security investments is to get funding. Another difficulty is to convince people to invest in certain things, e.g. top management. (Specialist#1)

The interviewer asked from the managers and specialists: *"What kind of financial calculations you utilize (e.g. ROI)?"* to which the manager#1 and specialist#1 explained that they make financial calculations (ROI+ROSI) for all cloud projects. The security side

also quantifies the economic significance of security risks in these calculations. Manager#1 also noted, that as with whole security industry, it is a challenge to quantify cost impact of security risks due tricky pricing. There is a need to do estimations on investments and security incidents impact for e.g. customers and the company. Specialist#1 explained that traditionally they used ROI for business case analysis in their department but sometimes ROSI was also used, thought it also can not exactly calculate return on investment due too many factors that need to be considered. Moreover, manager#1 continued to give an alternative way to approach security investment decisions that is used:

> *"Sometimes we use top down approach. The top management makes a conscious decision that it wants to increase the company's profile with information security. So, they decide to invest X amount of funds for example network infrastructure or information security training. There is no ROI calculation in the background these times."* (Manager#1)

Manager#2 however stated, that their particular organization/department does not have clear economic calculation formula usage when talking about risk monitoring and investments targeted towards that. Manager#2 elaborated that there is a need to *"go by our gut feeling"*. Specialist#1 also shared his opinion on alternative decision-making approach. There is a need to find consensus on what is the company's vision and where the IT is going. What parts need investment and what is important for the company e.g. in three years. Specialist#1, manager#1, and manager#2 all concluded, that it is difficult to convince people to invest in certain things and get funding for all IT projects.

Specialist#1 one was asked how he persuades his company to spend money on his security proposals. The short answer was through risk and threat analysis. He further elaborated that it is the only way to get funding for new processes and technologies. The process includes identifying possible threats and making risk analysis of them and their relevance to the company. With the analysis, inherent risk (worst case scenario) can be realized. Afterwards, what can be done about the inherent risk is considered, how much will it cost and how much can it be reduced. (Specialist#1)

Specialist#1 was also inquired, does he have a strategy how to persuade his company that it is important to spend money on his security proposals with an example. Speciliast#1 answered with a yes, the company has a cyber-security strategy, vision and related roadmap that seeks to get funding for future targets that they want to tackle. The roadmap shows where the company should invest in the future.

Understanding hackers

Relating back to game theoretic approach on security investments and technology selection, the managers were asked do they implement any strategies to identify potential hackers. Manager#2 thought that to be to targeted strategy. Hackers are not the biggest reason for security challenges. As a whole, security is much more than looking for hackers, due the background factors, such as individuals knowingly or accidentally causing security problems. Manager#2 argued, that he would not develop any straightforward hacker strategy, but a risk-based approach (identifying risks and weaknesses there). Manager#1 had a different view, representing different department. He explained, that like any major company, they have their own response teams who are constantly monitoring the network and the systems and are capable of intervening to any unusual transactions or if there are discrepancies in the network traffic. Manager#1 stressed that they have both internal and external ability to react for outside threats.

Interviewer continued to inquire, how effective or efficient the managers thought those strategies to be. Manager#1 believed them to be relatively effective, and continued to elaborate:

> *"The challenge is the continuous race between the attackers and defenders. The attackers come up with new tools and methods to stay more hidden in systems etc. Similarly, the defenders have to continuously update their own competence and if necessary, invest in new tools to identify these attacks."* (Manager#1)

Manager#2 also concurred, that many times companies are behind creating security strategies, and it is one of the most difficult challenges in information security. When thinking about information security evolution and how many weaknesses are uncovered daily, in a way the corporate culture (case organization) is dragging behind in this regard. There are more found weaknesses than you can patch.

4.4 Security policy compliance

ISS policy compliance and computer misuse is issue often attached to employees. In the interviews, the employee participants were first asked what they think are the most common ways security breaches (e.g. malicious software attacks) happen in their company. The answers varied between the interviewees and there were no real keywords to be picked, but the number one argumentation was the carelessness of the user (computer abuse, lack of compliance with set policies). This behavior, according to the interviewees, includes ignoring warnings you are given, taking shortcuts, sharing information with unauthorized people (confidentiality), and opening unknown email attachments (phishing and malicious code). It was also noted, that taking your computer outside of the internal network and using it e.g. home office, poses a risk of infection from the public internet. Employees therefore are aware of the user error element and humans being the weakest link in the ISS chain.

Security specialists had a different viewpoint on the question due their position and work they are tasked with. Two answers listed (spear) phishing attacks and brute force attacks as the most common reason, and one identified people as the most common factor: *"Careless employees upload classified material into a third-party service to ease file sharing"* (Specialist#2). He continued that he has rarely seen cases in which an organization has been breached though a network to extract information. The brute force attacks, according to specialist#1 are at present mostly targeted to cloud services and external, internet published on premise services. The spear phishing attacks are targeted attacks against individuals within their organization. As for the reasons for these, lack of funding and lack of proper user awareness are the reasons for successful attacks, according to specialist#1.

Interviewed security managers also listed information sharing through unapproved channels as most common way for security breaches to happen. Also, employees connecting company devices to insecure outside networks and browser plugin installations are common. These can result in malware infections. According to manager#1: "*Even with security training, users might accept these installations."* High quality communication attempts through email were also common for the organization to receive. For example, attacks against Office 365 systems were identified as quite common attack interfaces. Manager#2 stated, that they observe about 100 successful attack per week against the whole company.

When the employees were asked how well they think they follow security instructions set by the company, all of them were on consensus that to best of their knowledge, they do follow the security policies set by the company and do not think they ever break the rules and policies that are set. Employees were mostly however unsure, where they would be able to find security instructions or policies if they felt the need to review them at some point. Two of the security specialists also answered that they do comply with the policies (Specialist#1 stated that he personally writes them). One of the Security specialists answered with "fairly well" and continued with an elaboration that he just rechecked them during the week.

On a follow-up question, employees and security specialists were asked how well they think managers follow security instructions and set an example with their action. Employees did not have an opinion on how good an example managers make with their policy compliance, but three of them though that managers are capable and follow the instructions that are set by themselves. Employee#3 though that "*the security culture here is pretty good and the rules here make sense. There are no nonsense in the rules, so I think the managers abide them too."* Curiously, one of the employees though that the managers might not follow the policies that are set too well. Security specialists' opinions were aligned with employees. They too though that managers follow the set security instructions, but noted, that an exemplary behavior by the managers was not that strong with the current security culture.

Within organization, defined security policies can include variety of practices that need to be abided. These policies can include matters such as document handling and information sharing amongst subcontractors in terms of CIA. The employee interviewees were asked about what things relating to information and cloud security are they dealing with in daily basis, and do they find the measures they must take stressful or troublesome, or do they slow down their workflow. The answers included issues that the employees realized:

- Walking through doors (Restricting access to people without identification)
- Document classification system and sharing of those documents (personal, confidential, internal use)
- Physical internal documents are often moved off premises for remote working and sometimes left exposed
- Personal (public) cloud service usage for work documents
- Login credentials are required in multiple systems and interfaces
- Most of the services used are moved to cloud solutions and documents are stored in the cloud
- Remote accesses within the internal network and outside access to it (policies are set on how the connection is made)

Three of the four employees did not find the policies and practices they must follow stressful or time consuming. They further stressed that they think they are essential part of security that is maintained in the organization. One of the employees though that the especially the login process can slow him down if the credentials are lost or unavailable for time being. Getting the access to mandatory system may become hard, requiring phone calls and time.

Finally, regarding compliance with ISS policies, the employees were asked what they think are the pros and cons of complying with security instructions. Employee#1 thought that it is important that the company does not suffer financial loss due security incidents,

which in return helps to maintain employment. On the other hand, he stressed the importance of feeling secure:

> *"It also makes us feel safe in a company that has proper guidance's and security measures, so you can work securely. You don't get uncertain feeling about am I doing something wrong here and if so, is it a security risk? You should be confident in your work."* (Employee#1)

Employee#1 also though that the policies and measures should be easily available, since if they are hard to find in the internal network, nobody will even bother to check anything.

Employee#2 though complying with ISS policy is a good thing in order to prevent malware attacks. Employee#3 though that by complying with security rules and measure you do not have to fear for any sanctions if something happens. The measures have been formed by so called experts and there surely are reasons for their existence. He also did not believe that the company would implement any unnecessary policies. Employee#4 feared, that if the security instructions were not followed and something terrible would happen, he would be responsible. He felt that policies should be followed and there should not be soloing around.

When the managers were asked, do they think employees do not comply with set information security policies properly, both answered that they generally do follow the set policies and respect the security rules quite well. Manager#2 estimated that less than 10% of the personnel behave unexpectedly. Manager#1 reasoned that the situations when new employee comes in and despite the training, they might make a mistake in following the security policies.

4.5 Security policy development

It was clear that the case company had several security policies in various areas dictating how business and customer information was handled. The policies are also updated once a year. The managers were asked how they ensure employees and other related actors comply with set security policies. They listed various ways the company attempts to ensure compliance:

- Technical supervision (what is done with the company's own information systems)
- External controls (business documents cannot be found e.g. on the internet)
- Random audits
- Annual compulsory security training
- Policies are tested with company's own security testing

Manager#1 explained the random audits:

> *"Each year we select a number of functions and branches that are being audited with our audit function. We ensure that the company's business practices are in line with the regulations."*

In turn, manager#2 gave an example of the security testing:

> *"An example of this is kind of an organization-wide email phishing environment that we use to test how many people fall into such an email attack as it is one of our biggest risk interfaces."*

Both managers also stated, that a record is maintained on employees and other actor's prior knowledge on the policies when new ones are designed. In some branches of the organization, there are also training programs where a specific key person needs to reach e.g. level three in some security package. The progress of completion for each employee training is monitored.

In order to improve employee's compliance with set security policies, both managers had training as the number one method. There were however also other measures that the organization takes:

> "*We have a training environment, a model for identifying non-desired practices, and further training programs. Certain things and practices are even classified as punishable in our network. There even is a possibility of termination of employment if one behaves inappropriately."* (Manager#2)

The other manager elaborated on the nature of the training by explaining that lots of targeted training is conducted. Various organizations get tailored bundle of trainings that focuses on the work they are doing. The specific organizations perspective is used to talk about information security.

Interviewer also asked the security managers: *"Do you follow other company's policies or take guidelines from them? Can you give some kind of an example?"* Both managers answered with a definite yes. The case company has cooperation events all year round, they participate in active ISF system, through which they have few meetings a year and take guidance from. The company also has colleagues in various other companies around the world that they are in contact with to share thoughts, worries and solutions. Manager#1 also noted, that they track what are beginning to be standard in the industry and discuss with subcontractors and major clients about them. They actively follow and compare themselves to other businesses.

4.6 ISS awareness training

To address the compliance and misuse topic, IT security specialists and security managers tend to utilize security (awareness) training. Specialist#2 told that he personally hold a small-scale IT-security training. Other specialists were not directly involved with training tasks.

Considering the security managers, they were asked if they use security training programs (and what kind of) in their organizations, and how important they consider those training programs. Manager#1 illustrated the company's training program situation:

> *"There is basic training that is for everyone, and tailored training for people who have access to sensitive information or are dealing with, for example, information systems. In those situations where the security risk is emphasized, tailor-made packages are made for the involved people. For example, a system administrator will have a much deeper training than other employees. In addition, we have a very large library of other information security training through the company portal..."* (Manager#1)

The manager#1 thought the programs to be important, especially when security threats are changing, the training needs to keep up with new attack methods. Manager#2 also stated that the annual training is statutory, and it is important to maintain a certain baseline within the organization because staff comes and goes. If the annual training would be stopped, manager#2 estimated that it would appear as a surge in virus infections. Parameters would likely go worse and other data violations would surely increase. Manager#1 and #2 also explained that they maintain a record of employee's prior ISS knowledge when designing new training programs. Further, some branches of the company have specific key persons that need to reach a certain level of knowledge in some security packages.

Manager#2 also underlined that there are special volunteer courses, where one can seek and find more information about security. The company also has three-part expert training, where the trainee can collect three batches (security titles) based on how many of those additional trainings have been done. Employee#2 knew about the existence of mandatory training performed once a year and reasoned that all employees mostly receive instructions relating to security behavior though them. Interviewer continued to ask is the training held more than once a year if you could attend voluntarily, but the employee#2 had no knowledge of existence of voluntary training, only the mandatory one. When manager#2 was asked about this situation, he answered that the information can found on the home page of the company's internal portal. However, he estimated that still only about 50% of all employees are aware of the volunteer training courses.

4.7 The triad of cost, human and technology

After all the issues and topics were covered, the managers were asked about balance of social and technological factors:

> *"As you said earlier, to save money is important, to make sure employees understand the importance of security and comply with security policy is important, and to have the suitable technology is important, in your opinion, how do you sequence them (cost, human, technology)? Why?"* (Interviewer)

Manager#1 thought the question to be difficult to answer due the triangulation of the factors. If you cut in one place, other parts start to suffer. As an example, if you invest a lot in technology but there are no people to who are able to maintain it, the organization will do rather poorly. Manager#1 thinks that these factors should be in balance together, but the key factor is people. No extremes should be allowed, for example investing 100% to technology. Manager#2 had similar thoughts about the most important factor of this triangulation:

> *"A company cannot function without its personnel. Right people at right places are the most important thing in terms of information security. Technological tools are not now or in the future any more intelligent. So, we need capable personnel, who know to use right tools at right places."* (Manager#2)

Manager#2 also thought costs to be more important than technology at the current time, as technology expires so fast and leads to a cost spiral. When making organizations annual investment decision, technology already manages to expire within that year. Manager#2 argued that it is challenging to choose technology with a long lifecycle.

Manager#2 was also asked, do conflicts arise between cost, human and technology? He reasoned that at present, cost-effectiveness causes conflicts. This leads to a situation where risk mitigation becomes more difficult when cost savings are applied, leading into more risks.

5. Discussion and Implications

According to Alberts & Dorofee (2002), in order to improve overall information security within the company, security must be considered from multiple perspectives and continuous effort should be maintained to improve security posture. Companies increasingly face security risks and it becomes more and more important to create appropriate strategies to address the issues. The aim of this thesis is to answer the research question: *What are the factors that should be considered in order to improve information security in cloud computing?* To answer this, a case study of a large IT specialized company was conducted with semi-structured interviews. Employees, IT specialists and security managers were chosen as actors, each giving different perspectives to the issue of information security management. Employees represent the people; IT specialist's technology and the managers are dealing with the process aspect of the framework.

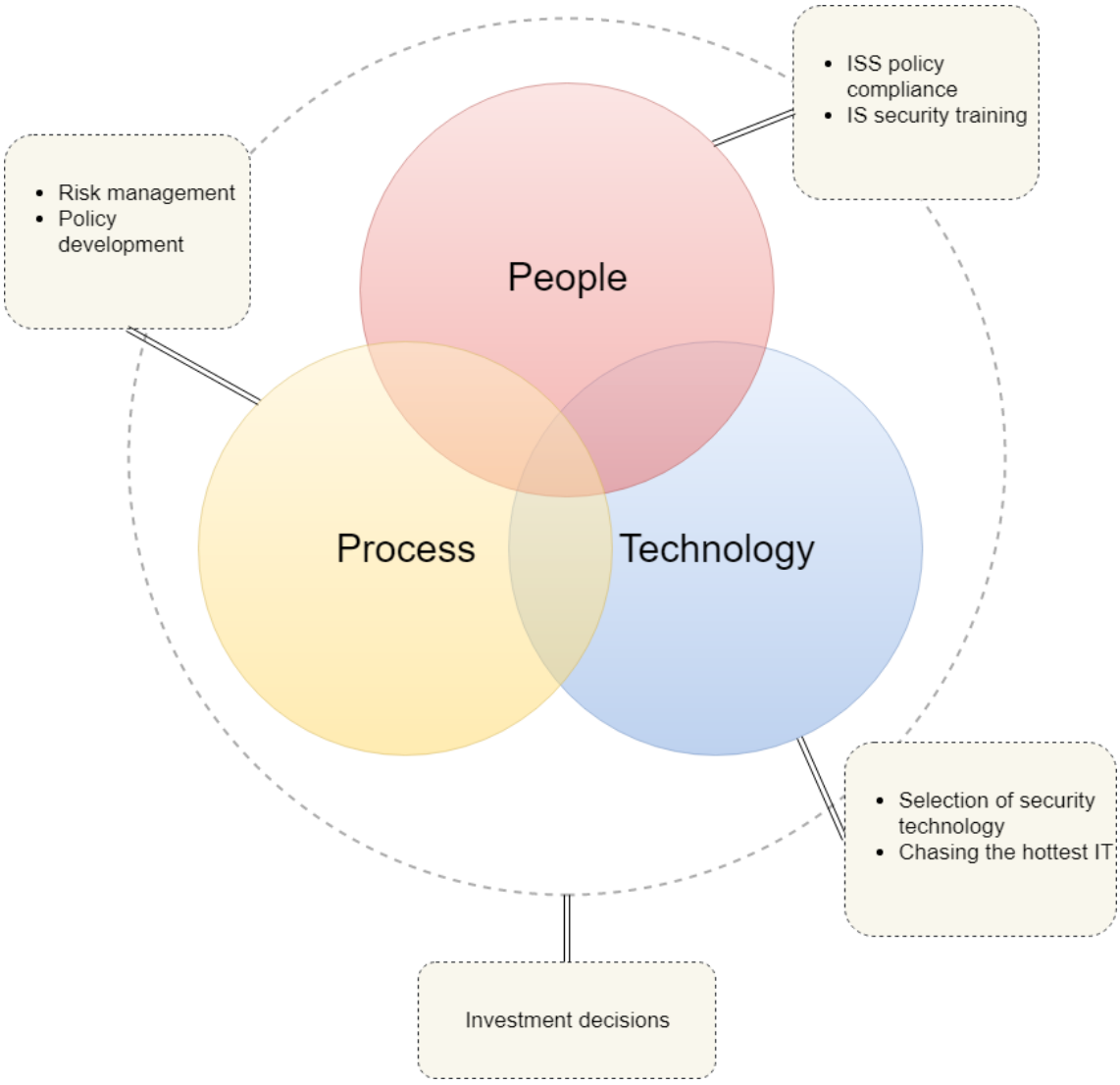

Figure 5. Adapted People, Process and Technology model

The adapted people, process and technology model illustrates how investment decisions directly affect all other covered topics that in turn have an effect to one another, forming 'information security'. The current research is discussed and compared to the prior literature on the topics, in relation to the research framework presented in Figure 5 (see above).

5.1 RQ 1.1: How is risk management conducted in an organization?

Risk management is a larger process consisting of sub activities which aim is to identify, evaluate and prioritize risks in order to create strategies and direct resources to minimize, monitor and control the probability of incidents that can happen causing e.g. financial loss for organization. Alberts & Dorofee (2002) advice to start with risk evaluation process, to get a baseline of organization's security status. Zhang et al., (2010) also concur with their risk management framework for cloud computing by suggesting starting with 'selecting relevant critical areas'. The risk management process (based on ISO/IEC 27001 standards) as a whole is conducted in following order (Zhang et al., 2010):

1. Selecting relevant critical areas
2. Strategy and planning
3. Risk analysis
4. Risk assessment
5. Risk mitigation
6. Assessing and monitoring program
7. Risk management review

After risk management review, the cycle reverts back to strategy and planning (Zhang et al., 2010). In the interviews, manager#1 explained the company's critical information protection program, where they indeed start by identifying what are the company's most critical data resources. According to the manager#1 they then continue to map out how the data resources and customer information are used and where, and by which stakeholders. The case company also classifies risk according to their value, where main risks are listed, and strategic plans are made (Manager#2). This corresponds to the second process suggested by Zhang et al., (2010).

For risk analysis, manager#2 introduced the ISF influenced guidance list (1-9) to calculate risks, which is used in certain departments of the company. Further, the case company has set different levels of risk probability that are used in analysis: e.g. low, medium and high. Another interesting notion is that there was no mention of utilizing Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) approach in the studied case company, although suggested by Alberts & Dorofee (2002) and Zhan et al., (2010) to do risk evaluation and analysis.

Risk assessment is the output of risk analysis with four key processes: likelihood determination, impact analysis, risk determination and control recommendations (Zhang et al., 2010). It was clear that risk analysis in the case company included vulnerability identification (scanning) and specialist#2 personally carried out this activity. The case company also categorized the risks to primary and secondary. Primary risks are what directly affects production, and secondary risks that affect sales indirectly (primary and secondary loss).

Zhan et al., (2010) noted that due the multiple different models of cloud computing available, there are also various ways to create a risk treatment plan (RTP). This can have functions such as avoidance, transfer, retention, reduction and acceptance (residual risk). There were no detailed explanation of the usage of these risk treatment functions except the reduction and acceptance functions, which were discussed in the interviews. The mitigation status is actively monitored by the case company: the extend of the risks that could affect the critical data sources and the schedule they should be closed down. There is also formal risk acceptance process for residual risk and its acceptance.

Assessing and monitoring program can incorporate e.g. internal audits, according to Zhang et al., (2010), and indeed manager#1 explained that when assessing the CSP, three level model is utilized: requirement formulation, basic supplier screening, and technical inspections such as on-site audits. This follows the process introduced by Zhan et al., (2010). The case company also uses incident management process in order to react to incidents.

As shown, the risk management process the case company follows has many similarities in the structure Zhang et al., (2010) suggests it to be in cloud computing setting. With cloud computing, there are also multiple parts that differ from traditional risk management conducted in organization, e.g. the CSP relation, which brings additional consideration into play for organizations.

5.2 RQ 1.2: What are the key factors while selecting security technologies?

The interviews revealed multiple factors and considerations that are important to the case company on cloud technology selection and investments: usage of standards as a security baseline, interoperation and integration, joint manageability, cost effectiveness, vendor lock-in, vendor reputation, scalability of solutions, and geolocation of the services (see Table 2). Radack (2004) also found comparing costs and features of different solutions important, in addition to reviewing the compatibility with existing systems. Other factors important for organization to consider are total life cycle costs, ease of use, scalability, and product vulnerabilities. Tang & Liu (2015) also considered the importance of interoperability, security governance (preventing vendor lock-in) and legislative concerns, relating mostly to the issue of geolocation that the case company needs to consider when information is exported to different countries.

There was no indication of usage of any specific decision model, falling back to the knowledge, experience and general good practices that are used within the case company when selecting security technologies. The case organization prefers to use standards as a baseline security, possibly relating to the issue of how difficult it becomes to compare different technologies when the investment dimension is added.

Selecting right security technologies can be difficult in cloud computing setting due the uncertainty that is attached to ISS. The inability to reach a decision can lead to herding behavior within managers. The behavior is influenced by reputation, that especially managers attempt to maintain, and when facing uncertainty in investment decision or technology selection, they tend to make decisions based on others. (Shao et al., 2019) The inability to accurately compare cost and benefit for organizations can be a reason why the usage of cost benefit analysis is not popular approach for selecting security technologies.

Based on the interviews, there was no evidence of tendency to gravitate towards herding behavior while reviewing and selecting different technology solutions in the case company. Organization may consider that it is safer to implement a generally adopted existing security baseline, e.g. based on ISO-27001 standard or ISC checklists, due the uncertainty factor.

Costs and usability are also important. The empirical data and prior literature shows that organizations prefer to have easy to use systems with joint manageability, meaning that e.g. implemented cloud products are managed from single interface or system. This reduces the complexity that large cloud solution packages can introduce to companies

with existing systems that require interoperability. Lastly, as literature also recognizes in addition to the constant appearance in the interviews, costs most of the time play the most important role on the selection process.

5.3 RQ 1.3: In what investment decisions are based upon?

The literature suggests invoking game theory or decision analysis models to reach decision on strategic investments. More elaborated variations of decision analysis are value-at-risk approach and cost-benefit analysis. For managers however, it difficult to utilize cost-benefit analysis in practice, since there is no way to create reliable actuarial loss statistics or have historical data in order to make predictions. (Shao et al., 2019; Gordon & Loeb, 2006) Instead of relying on pure economic calculations, managers might need to rely on recommendations from experts or follow processes used by other organizations (Shao et al., 2019). Gordon & Loeb (2006) also suggest that security managers can use last year's budget and best practices of the industry as a factor for IS budgeting.

Based on the interviews, it appears that the case company favors the usage of economic calculations compared to utilization of game theory on investment decisions. As specialist#2 explained, that for a company that's purpose is to make money for its owners, a positive business case has to be calculated. The case company prefers to use ROI and ROSI calculations for its cloud projects, while the security side also quantifies the economic significance of security risks in these calculations. The specialist#1 also noted that the usage of ROSI calculation is tricky and exact return on investment value cannot be calculated due the multitude of factors. The output therefore is a calculated estimation. This is also what Shao et al., (2019) and Gordon & Loeb, (2006) agree on the uncertainty that surrounds information security and related investments. Furthermore, this model of decision-making correlates with how Gordon & Loeb (2006) suggest cost-benefit analysis can also be used: reduce weight on formal quantifiable benefits, and use modified economic models, considering potential losses from security breaches.

The second and alternative way that the case company sometimes makes investment decision is a top down approach. As described: the top management makes a conscious decision that it wants to increase the company's profile with information security. So, they decide to invest X amount of funds for example network infrastructure or information security training. No ROI calculations are used in these situations. This style of investment decision making was not suggested by the examined prior literature. There are however some reasons for company to decide to increase its profile on information security. As an example, the company might be responding to acquired bad publicity due recent security incident a company might have sustained.

The third way to make investment decisions in the case company is similar to the top down approach. Specialist#1 explained that the company finds a consensus on the company's vision and the direction the IT is going. Based on this, important future goals for the company (e.g. in three years) are mapped and after processing some are proposed as investment targets in the roadmap.

There was no indication of game theory utilization with the case company when directly asked about the investment decisions. However, when hackers were introduced as vector in the interviews, Manager#1 explained that the challenge in investments and security strategies is the continuous race between the attackers and defenders. The attackers come

up with new tools and methods to stay more hidden, while the defenders have to continuously update their own competence and if necessary, invest in new tools.

These findings correlate to the explanation by Cavusoglu et al., (2008) and Herbert & Yao, (2008) of game played between the company and the hacker in this instance. No indication can be drawn on the specifics of the game, e.g. is the game scenario simultaneous or sequential.

5.4 RQ 1.4: How are ISS policies developed and managed?

One aspect of ISS policy management is how the managers ensure the employees compliance with the set policies. The case company utilizes various methods to ensure compliance: technical supervision, external controls, random audits, annual compulsory security training, and testing the developed policies. The random audits are conducted annually within the target company to ensure the company's business practices are in line with regulations. Niemimaa & Niemimaa (2017) recognized this being one reason originations adopt standards and best practices of the industry. The case company also tests the developed policies with their own security testing. As an example of this testing is an organization-wide email phishing environment that the company uses to attempt email phishing attacks towards the organization's personnel.

The case company cooperates and participates in active ISF system, from which they take guidance from (standards and best practices). They also have connections and colleagues in various other companies globally, to with thoughts, worries and solutions are shared with. So, in essence the case company also follows other companies and takes guidance from them.

According to Niemimaa & Niemimaa (2017) and Wiander (2007) the implementation of ISS practices and policies should be done in such a way that they become part of existing practices and are performable by the employees. In other words, they should be implemented in the daily activities of the organization. The specific contents and details of the policies in use within the case company was not in the scope of the thesis and therefore no deduction on this can be drawn from the empirical data.

5.5 RQ 1.5: What affects employee's policy compliance?

There is extensive prior research done in regards of information security policy compliance in varying organizational settings. It has been proposed, that employees are not always motivated to follow set security policies and instructions and have tendency to follow their habits and routines and being resistant to behavioral changes (Chen et al., 2012). ISS violations can also be caused by employees' negligence or ignorance of set policies (Siponen & Vance, 2010). Many theories attempt to explain the behavior regarding policy compliance: e.g. deterrence theory, neutralization theory, rational choice theory, and protection motivation theory. Literature also introduces different ways to enforce compliance in forms of coercive remunerative and normative control mechanisms (Chen et al., 2012).

The interviews showed that the computer misuse and negligence of set policies do happen in the case company. The behavior includes ignoring warnings you are given, taking shortcuts, sharing information with unauthorized people (confidentiality), and opening unknown email attachments (phishing and malicious code). The interviewees reasoned

that this comes down to convenience. Specialist#1 reasoned, that the behavior could also be caused by lack of proper user awareness and lack of funding to better it.

It became clear that the employees were aware of the user error element and humans being the weakest link in the ISS chain. They also thought that they themselves, to best of their knowledge do not break the set policies and rules. Neutralization theory could explain some of these cases: person breaking organization's security policies justifies his actions in the moment by claiming (to oneself) that no actual harm will be done. (Siponen & Vance, 2010; D'Arcy et al., 2014).

Another point found in the interviews was that the employees thought following and complying with ISS policies is a good thing. This was because of the fear of sanctions that they might face if a security incident happens (Employee#3; Employee#4). This behavior correlates to protection motivation theory, where individuals are motivated to react to warnings, threats and dangers and their behaviors elicited as a response to a fear appeal.

ISS training as countermeasure

Prior literature suggests training as the number one method to counter the problem of employee's non-compliance and to enhance employee's security awareness (Karjalainen, 2011; Puhakainen & Siponen, 2010; Hsu, 2009). In other words, security training plays a key role in ISS policy management, since the people can be considered the weakest link in information security due the majority of security incidents are caused by them unintentionally or intentionally.

The case company has the aforementioned compulsory annual training, but also organize voluntary training programs and maintain the training environment. This environment is a model for identifying non-desired practices and further the training programs. In addition to the voluntary training, specific persons within the company have tailored training programs who have access to sensitive information or information systems. As an example, a system administrator has much deeper training than others due the emphasized security risk situation.

This description correlates to Puhakainen & Siponen (2010) implications, that successful ISS policy compliance training program should consider the target's (e.g. employee) previous knowledge on the subject and they should be tailored to be relevant to the learner. Moreover, the training carried out in the organization should be continuous activity instead of one-time session, to increase compliance further.

It is mandatory to maintain and adapt training programs because security threats and attack methods are changing, and staff is altering within the company. Without compulsory training, manager#2 estimated that it would show as surge of virus infections and other data violations.

5.6 RQ 1.6: How is IT fashion related to IS security in cloud computing?

Wang (2010) argued that IT fashion influences organizations performance, reputation and executive compensation. Following the hottest it can also legitimize organizations regardless of their performance. The interviews did not yield any concluding assumptions that could be drawn on the effects of IT fashion or the phenomenon of chasing the hottest

IT. There was no specific mentioning on being early adopter or investing in something that is considered ‘being in fashion’ right now. Further research is required to draw implications on the effects of these concepts.

5.7 Theoretical implications

This study provides a unique perspective to information security management by inspecting the rising concept of cloud computing from three perspectives: people, process and technology. Previous frameworks for security management in organizations have included aspects such as technology and processes. To gain insight into the issue from the third perspective in a same study, three different actors were chosen to provide the points of view into the research problem. As the study shows, information security is not only about technical aspects (e.g. cloud solutions) but also about social factors, the people who use the systems.

Traditionally (simplified) risk management is about calculating risks and returns. When introducing information security into the process, calculating becomes difficult due the uncertainty that is attached to ISS. For practice, future research should ask the question: what is needed to make such investment decisions? Should certain formulations be used or something entirely different?

It also became clear in the study that the phenomenon of chasing the hottest IT and IT fashion could be explored more in future studies and its appliance to the specific context of cloud security. Is it relevant and does it have an effect on information security management?

5.8 Managerial implications

There are multitude of things that companies and managers can consider when carrying out information security management in the cloud computing setting. First, there is no need to stress about specific calculations on investment decisions because it is really hard to do (uncertainty factor). As solution, one can just follow others or industry’s best practices. Managers can also think of other methods beside financial calculations to do security management.

As people are the most common cause for occurring security incidents, ISS policies are one of the most important ways to control people’s security behavior. Managers need to make policies visible and easily accessible to employees (improving compliance). The policies and definitions should also be in line with other business activities. In addition, the whole security concept needs to be in line with the company’s business model. There should not be cases where information security organization defines how security should be done but is in conflict with rest of the organization’s goals and practices.

ISS training also plays a key role in security management and is one way to counter the employee’s non-compliance towards set policies and practices. Deep enough security knowledge should be maintained with appropriate stakeholders within the company, since people are the weakest link in security.

6. Conclusions

The purpose of this thesis was to give suggestions and more holistic perspective for organizations and management on information security in cloud computing setting. This research is first one to inspect the problem from three different perspectives in one study: people, process and technology. The empirical data was collected from the selected case company with three different actor categories: employees, IT security specialists, and security managers. Each of the actors give a unique viewpoint to the research problem. Findings from the empirical data were compared and discussed with prior research conducted on seven selected issues and topics related to information security management.

This study attempted to answer the research question of *"What are the factors that should be considered in order to improve information security in cloud computing?"* through the constructed supporting research questions. The research results show that the problem of information security management is dependent on many factors, some more important than others. Together with considerations on investment decisions, security technology selection, policy development and implementation, ISS training, risk management and ISS policy compliance assurance, can effective security posture be achieved and maintained within an organization. The argumentation stands, that information security is not only about technical aspects (e.g. cloud solutions) but also about social factors, the people who use the systems. These factors are for example human behavior, compliance and attitudes towards ISS policies, and received training and knowledge.

Research results show how risk management, investment decisions, technology selection, ISS training, ISS policy development and implementation are conducted in today's large ICT oriented company. In addition, what affects employee's policy compliance and how it can be improved were discussed. This study contributes to the community by attempting to give a holistic perspective on information security management in the specific setting of cloud computing. The adapted people, process and technology model illustrates how investment decisions directly affect all other covered topics that in turn have an effect to one another, forming 'information security'.

6.1 Limitations of the study and future research

This study can be considered to be quite horizontal, as it does not dive very deep into any particular topic or issue that was introduced. It only scratches the surface on the inspected larger topic. Another major issue is that the study is confined by having only one case company as source of empirical data, and therefore generalization of the results cannot be considered very feasible.

Furthermore, qualitative interviews can have tendency to incorporate typical limitations and problems such as lack of trust, time pressure, elite bias, and ambiguity of language (Myers & Newman, 2007). These issues may well have affected the output of the study to some extent, especially when interviewees were asked about sensitive topics related to security or their own performance.

Discussion and presentation of earlier research on the topic of ISS policy compliance was left partial due the scope of the research. Not all of the explaining theories on compliance (11) could be introduced as Moody et al., (2018) did. Only few were selected in the previous study section, regarding employee's security policy compliance.

Lastly, the study did not reach to any meaningful results on the issue of chasing the hottest IT and IT fashion, leaving its relevance and effect on information security management open in this instance. Future research could look into to the topic, if IT fashion and the phenomenon of chasing the hottest IT influences organizations performance, reputation and executive compensation as Wang (2010) argues. Also, is the topic relevant and does it influence information security management?

As already introduced, further recommendations for future research involves risk management; calculating risks and returns. When introducing information security into the process, calculating becomes difficult due the uncertainty that is attached to ISS. For practice, future research should ask the question: what is needed to make such investment decisions? Should certain formulations be used or something entirely different?

References

Abed, J., & Weistroffer, H. R. (2016). Understanding deterrence theory in security compliance behavior: a quantitative meta-analysis approach. *SAIS 2016 Proceedings. Retrieved from http://aisel.aisnet.org/sais2016/28*.

Adams, J (2017). Forrester Data: Cloud Security Solutions Forecast, 2016 To 2021 (Global). Retrieved from https://www.forrester.com/report/Forrester+Data+Big+Data+Management+Solutions+Forecast+2016+To+2021+Global/-/E-RES135913

Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*, *6*(1), 25.

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

Andress, A. (2003). *Surviving security: how to integrate people, process, and technology*. Auerbach Publications.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft cloud computing synopsis and recommendations. *NIST special publication*, *800*, 146.

Barlow, J., Warkentin, M., Ormond, D., and Dennis, A. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," Computers & Security (39: Part B), pp. 145-159

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, 369-386.

Cavusoglu, H., & Raghunathan, S. (2004). Configuration of detection software: A comparison of decision and game theory approaches. *Decision Analysis*, *1*(3), 131-148.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87-92.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, *25*(2), 281-304.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability and Security* (pp. 546-555). IEEE.

Cherdantseva, Y., & Hilton, J. (2015). Information security and information assurance: discussion about the meaning, scope, and goals. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (pp. 1204-1235). IGI Global.

Chou, T. Y., Seng-cho, T. C., & Tzeng, G. H. (2006). Evaluating IT/IS investments: A fuzzy multi-criteria decision model approach. *European Journal of Operational Research*, *173*(3), 1026-1046.

Curiac, D. I., & Pachia, M. (2015). Controlled information destruction: the final frontier in preserving information security for every organization. *Enterprise Information Systems*, *9*(4), 384-400.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Fichman, R. G. 2004. "Going Beyond the Dominant Paradigm for Information Technology Innovation Research: Emerging Concepts and Methods," Journal of the Association for Information Systems (5:8), pp. 314-355.

Gordon, L. A., & Loeb, M. P. (2006). Information Security Expenditures. *Communications of the ACM*, *49*(1), 121.

Hasan, M. Y. F. (2011). *A New Approach for Sensitive Data Leakage Prevention Based on Viewer-Side Monitoring* (Doctoral dissertation, Al-Balqa'Applied University).

Herbert, J. P., & Yao, J. (2008, May). Game-theoretic risk analysis in decision-theoretic rough sets. In *International Conference on Rough Sets and Knowledge Technology* (pp. 132-139). Springer, Berlin, Heidelberg.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140-150.

Inukollu, V. N., Arsi, S., & Ravuri, S. R. (2014). Security issues associated with big data in cloud computing. *International Journal of Network Security & Its Applications*, *6*(3), 45.

Karjalainen, M. (2011). Improving Employees' Information Systems (IS) Security Behavior-Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees' IS Security Behavior. *PhD. University of Oulu*.

Kayworth, T., & Whitten, D. (2012). Effective information security requires a balance of social and technology factors.

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, *32*(5), 232-240.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & management*, *41*(6), 707-718.

Leighon, T. (2009). Akamai and cloud computing: A perspective from the edge of the cloud (White Paper). Akamai Technologies.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001, June). A model for information assurance: An integrated approach. In *Proceedings of the 2001 IEEE workshop on information assurance and security* (Vol. 310). United States Military Academy, West Point. IEEE.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE. *MIS Quarterly*, *42*(1).

Morsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Myers, M. D. (2013). *Qualitative research in business and management*. Sage.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1-20.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, *2*(1), 1-28.

Pettigrew, A. M. (2013). The Conduct of Qualitative Research in Organizational Settings. Corporate Governance: An International Review, 21(2), 123-126. 2

Pope, C., Ziebland, S., & Mays, N. (2006). Analysing qualitative data. *Qualitative research in health care*, 63-81.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In *Computational Intelligence and Networks (CINE), 2015 International Conference on* (pp. 116-123). IEEE.

Radack, S. (2004). *Selecting Information Technology Security Products* (No. ITL Bulletin April 2004). National Institute of Standards and Technology.

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, *16*(1), 69-73.

Ristov, S., Gusev, M., & Kostoska, M. (2012, May). A new methodology for security evaluation in cloud computing. In *2012 Proceedings of the 35th International Convention MIPRO* (pp. 1484-1489). IEEE.

Rogers, E. M. 2003. Diffusion of Innovations (5th ed.), New York: Free Press.

Seaman C. (1999) Qualitative Methods in Empirical Studies of Software Engineering. IEEE Transactions on Software Engineering 25(4): 557-572.

Securosis, L. L. C. (2010). Understanding and Selecting a Data Loss Prevention Solution. *Securosis, LLC, [Online]. Available: https://securosis. com/assets/library/reports/DLP-Whitepaper. pdf*. (Accessed on: January 24, 2019)

Sen, J. (2015). Security and privacy issues in cloud computing. In *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1585-1630). IGI Global.

Shao, X., Siponen, M., & Pahnila, S. (2019, January). To Calculate or To Follow Others: How Do Information Security Managers Make Investment Decisions? In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), 45.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, *22*(1), 77-94.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security*, *50*, 60-73.

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource*. John Wiley & Sons.

Teh, P.-L., Ahmed, P. K., and D'Arcy, J. (2015). "What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory," Journal of Global Information Management (23:1), pp. 44-64.

Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *The Journal of Strategic Information Systems*, *23*(2), 174-186.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating ISS compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. *IEEE transactions on Services Computing*, *5*(2), 220-232.

Wang, P. (2010). Chasing the hottest IT: Effects of information technology fashion on organizations. *MIS quarterly*, *34*(1).

Wiander, T. (2007). Positive and negative findings of the ISO/IEC 17799 framework. *ACIS 2007 Proceedings*, 75.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In *2010 10th IEEE international conference on computer and information technology* (pp. 1328-1334). IEEE.

Appendix A. Interview forms - English

Background information for all

Interviewer: Joni Penjala
Interviewee: -
Interview setting and time: Interview conducted in...
Affiliation with interviewee:
Interviewee age:
Education:
Work experience:
Usage of voice recording devices: Y/N (have to ask)

Employee

Questions

Interviewer introduces himself and explains the purpose of the interview.

1. What are in your opinion the most common ways security breaches (e.g. malicious software attacks) happen in your company?
2. How well do you consider you personally follow security instructions set by your company?
3. How well do you think managers follow security instructions and set an example?
4. What things, you consider information security, are you dealing with daily basis? What things more rarely? Are there any cloud security related ones?
5. What other security issues you consider important for your work?
    a) Do you find the measures you must take stressful or troublesome? (*compliance)*
    b) Do you think the measures slow down your work in a meaningful amount?
    c) Do you think some of these measures are unnecessary?
    d) Would you like to see changes made to these security measures?
6. Generally, what do you personally think are the pros and cons of complying with security instructions?
7. How would you rate (1-5), how well your company manages their information security overall? [1: poor, 5: excellent]

IT security specialist

Questions

Interviewer introduces himself and explains the purpose of the interview.

1. What are in your opinion the most common ways security breaches (e.g. malicious software attacks) happen in your company?
2. How does cloud security differ from on-premises security?
3. How well do you consider you personally follow security instructions set by your company?
4. How well do you think managers follow security instructions and set an example?

5. What factors affect possible security investments?
    a) What kind of risk assessment do you do?
    b) What kind of financial calculations you utilize (e.g. ROI)?
    c) Other ways to make decision on security investment?
6. As a security specialist, what do you consider when you select security technology for your company?
7. What are the obstacles when you recommend/implement security technology for your company? (after they share something, you can continue ask if the obstacles come from managers (higher level management), or from employees' non-compliance)
8. How would you rate (1-5), how well your company manages their information security overall? [1: poor, 5: excellent]
9. In general, how do you persuade your company that it is important to spend money on your security proposals (for example, spending some money on new technology, or launching new employee security training, etc.)?
10. When you propose your suggestions, do you use any metrics (for example, ROI, ROSI, cost-benefit analysis, or whatever else)?
11. Do you have any strategy to persuade your company that it is important to spend money on your security proposals? Can you provide some example?

Security manager

Questions

Interviewer introduces himself and explains the purpose of the interview.

1. What are in your opinion the most common ways security breaches (e.g. malicious software attacks) happen in your company?
2. As a security manager, what in your opinion are important factors to pay attention to in information security management?
3. As a security manager, what in your opinion are the obstacles when you do information security management?
4. Do you follow other company's policies or take guidelines from them? Can you give some kind of an example?

Part 1: Security technology investment

5. How does cloud security strategy differ from on-premises security strategy?
6. What do you consider when you select cloud security technology for your company? Can you give an example?
7. What factors affect possible security investments?

a. What kind of risk assessment do you do?
b. What kind of financial calculations you utilize (e.g. ROI)?
c. Other ways to make decision on security investment?

8. What are the obstacles when you implement security technology for your company? (after they share something, you can continue ask if the obstacles come from managers (higher level management), or from employees' non-compliance)

Part 2: Security policy development

9. Do you have security policies set in the organizations that needs to be followed?

10. How do you ensure employees and other related actors comply with set security policies?
11. Do you think employees do not comply with set information security policies properly? Why?
12. What measures do you take that improves employee's compliance with set security policies?
13. Do you maintain record on employees and other actor's knowledge on previous policies when designing new ones?

Part 3: ISS awareness training

14. Do you use security training programs in your organizations? What kind of?
a. How important you consider these training programs?
b. Is the training continuous or for example annual?

Part 4: Risk management

Rest of the questions are cut.

Appendix B. Interview forms - Finnish

Taustatietoa

Haastattelija: Joni Penjala
Haastateltava: -
Paikka ja aika: Interview conducted in...
Tunteeko haastateltava haastattelijan:
Haastateltavan ikä:
Koulutus:
Työkokemus:
Haastattelun äänitys: Kyllä/Ei (kysy)

Työntekijä

Kysymykset

Haastattelija esittelee itsensä ja kertoo haastattelun tarkoituksen

1. Mitkä mielestänne ovat yleisimmät tavat, miten tietoturva rikkomuksia (kuten haittaohjelma hyökkäykset) tapahtuu organisaatiossanne?
2. Kuinka hyvin koet itse seuraavasi yrityksenne asettamia tietoturva ohjeistuksia?
3. Kuinka hyvin uskot johtoportaan seuraavan tietoturva ohjeistuksia ja ovatko he esimerkillisiä toiminnassaan?
4. Minkä seikkojen kanssa, jotka koet olevan sidoksissa tietoturvaan, olet tekemisissä päivittäin?

a. Entä pilviturvallisuuteen?

5. Mitä muita tietoturvaan liittyviä asioita koet olevan tärkeitä työssäsi?

. Ovatko näihin asioihin liittyvät käytännöt stressaavia tai hankalia?

a. Koetko että nämä käytännöt hidastavat työntekoa merkittävästi?

b. Uskotko joidenkin näistä käytännöistä olevan turhia?

c. Haluaisitko nähdä muutosta näissä tietoturva käytännöissä?

6. Yleisesti, mitkä koet olevan tietoturvaohjeistuksen noudattamisen hyvät ja huonot puolet?
7. Asteikolla 1-5, kuinka hyvin koet, että yrityksesi hallinnoi omaa tietoturvaansa? (1 huonoin, 5 paras)

IT tietoturva spesialisti/asiantuntija

Kysymykset

Haastattelija esittelee itsensä ja kertoo haastattelun tarkoituksen

1. Mitkä mielestänne ovat yleisimmät tavat, miten tietoturva rikkomuksia (kuten haittaohjelma hyökkäykset) tapahtuu organisaatiossanne?
2. Kuinka pilvitietoturva eroaa paikallisesta (on-premise) tietoturvasta?
3. Kuinka hyvin koet itse seuraavasi yrityksenne asettamia tietoturva ohjeistuksia?

4. Kuinka hyvin uskot johtoportaan seuraavan tietoturva ohjeistuksia ja ovatko he esimerkillisiä toiminnassaan?
5. Jos mietit työtehtävääsi tietoturva asiantuntijana, mitä asioita mietit, kun valitset yrityksellesi tietoturva teknologioita?
6. Mitä vaikeuksia ja esteitä nousee esille, kun suosittelet tai implementoit tietoturvatekniikkaa yrityksessäsi? (Kun jotain asioita on mainittu, kysy -> tulevatko esteet johtoportaalta vai muiden työntekijöiden vastustuksesta?
7. Asteikolla 1-5, kuinka hyvin koet, että yrityksesi hallinnoi omaa tietoturvaansa? (1 huonoin, 5 paras)
8. Yleisesti, miten vakuutat yrityksesi, että on tärkeää käyttää rahaa tietoturva investointeihin? (Esimerkiksi uusiin teknologioihin tai luoda uusia koulutusohjelmia työntekijöille)
9. Kun esität tietoturvaan liittyviä ehdotuksia, käytätkö mitään metriikoita, esimerkiksi ROI:ta, ROSI:a, kustannus-hyötyanalyysiä tai muuta?
10. Käytätkö mitään strategiaa millä vakuutat yrityksesi käyttämään rahaa tietoturvainvestointeihin? Voitko antaa esimerkkejä?

Tietoturvapäällikkö

Kysymykset

Haastattelija esittelee itsensä ja kertoo haastattelun tarkoituksen

1. Mitkä mielestänne ovat yleisimmät tavat, miten tietoturva rikkomuksia (kuten haittaohjelma hyökkäykset) tapahtuu organisaatiossanne?
2. Tietoturvapäällikkönä, mitkä ovat mielestäsi tärkeimmät faktorit mitä tulee ottaa huomioon tietoturvan hallinnassa.
3. Tietoturvapäällikkönä, mitä esteitä kohtaat tietoturvan hallinnassa?
4. Seuraatko muiden organisaatioiden tai yritysten policyitä/menettelyitä tai otatteko niistä esimerkkiä? Voitko antaa esimerkkejä?

Osa 1: Tietoturvateknologia investoinnit - Information Security investments

5. Kuinka pilvitietoturvastrategia eroaa ’on-premises’ tietoturvastrategiasta?
6. Mitä asioita harkitset, kun valitset yrityksellesi pilvipalveluiden tietoturvateknologioita? Voitko antaa esimerkkejä?
7. Mitkä faktorit vaikuttavat mahdollisiin tietoturvainvestointeihin?

A. Minkälaisia riskianalyysejä teette?
B. Minkälaisia talouslaskelmia teette? (Esimerkiksi ROSI)
C. Onko muita tapoja tehdä tietoturvainvestointipäätöksiä?

8. Minkälaisia esteitä kohtaat, kun implementoit tietoturvateknologioita yrityksellesi? (Tulevatko nämä esteet työntekijöiden vastahakoisuudesta?)

Osa 2: Security policy development Tietoturvaohjeistusten/tietoturvapolitiikan kehittäminen

9. Onko organisaatiossanne tietoturvakäytäntöjä (policyitä), joita tulee noudattaa?

10. Kuinka takaatte, että työntekijät ja muut sidosryhmät noudattavat asetettuja tietoturvakäytäntöjä?
11. Luuletko että työntekijät eivät noudata asetettuja tietoturvakäytäntöjä kunnolla? Miksi?
12. Mitä toimenpiteitä teette, jotka parantavat työntekijöiden tietoturvaohjeistuksien noudattamista? (improve compliance)
13. Pidättekö kirjaa työntekijöiden ja muiden sidosryhmäläisten nykyisestä tieto tasosta, kun suunnittelette uusia tietoturvaohjeistuksia/käytäntöjä?

Osa 3: ISS awareness training - Tietoturvakoulutukset

14. Onko organisaatiossanne käytössä tietoturvakoulutuksia? Minkälaisia?
a. Kuinka tärkeänä näet nämä koulutusohjelmat?
b. Onko koulutus jatkuvaa vai esimerkiksi vuosittaista?

Rest of the questions are cut.